98P1764

PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6: H04L 9/08 B1 A1

(11) Internationale Veröffentlichungsnummer: WO 96/37064

(43) Internationales Veröffentlichungsdatum: 21. November 1996 (21.11.96)

(21) Internationales Aktenzeichen: PCT/DE96/00835

(22) Internationales Anmeldedatum: 13. Mai 1996 (13.05.96)

(30) Prioritätsdaten:

195 18 546.3	19. Mai 1995 (19.05.95)	DE
195 18 545.5	19. Mai 1995 (19.05.95)	DE
195 18 544.7	19. Mai 1995 (19.05.95)	DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D-80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: HORN, Günther [DE/DE]; Eduard-Schmid-Strasse 16, D-81541 München (DE). MÜLLER, Klaus [DE/DE]; Raintaler Strasse 15, D-81539 München (DE). KESSLER, Volker [DE/DE]; Pfarrer-Schmitter-Strasse 1, D-85256 Vierkirchen (DE).

(81) Bestimmungsstaaten: CN, JP, US, europäisches Patent (AT BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC NL, PT, SE).

Veröffentlicht

Mit internationalem Recherchenbericht.

Vor Ablauf der für Änderungen der Ansprüche zugelassene Frist. Veröffentlichung wird wiederholt falls Änderunge eintreffen.

(54) Title: PROCESS FOR THE COMPUTER-CONTROLLED EXCHANGE OF CRYPTOGRAPHIC KEYS BETWEEN A FIRST ANI A SECOND COMPUTER UNIT

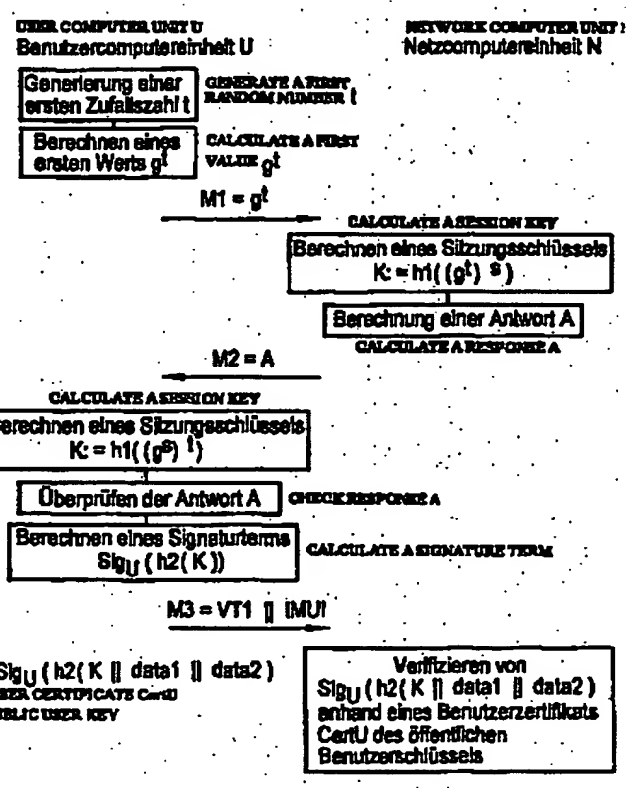
(54) Bezeichnung: VERFAHREN ZUM RECHNERGESTÜTZTEN AUSTAUSCH KRYPTOGRAPHISCHER SCHLÜSSEL ZWISCHEN EINER ERSTEN COMPUTEREINHEIT UND EINER ZWEITEN COMPUTEREINHEIT

(57) Abstract

The invention relates to a process by means of which a session key (K) can be agreed upon between a first computer unit (U) and a second computer unit (N) while preventing unauthorised third parties from obtaining useful information concerning the key or the identity of the first computer unit (U). This is achieved by embedding the principle of the E1-Gamal key exchange into the process of the invention with additionally by the formation of a digital signature via a hash value of the session key (K) generated by the first computer unit (U).

(57) Zusammenfassung

Die Erfindung betrifft ein Verfahren, mit dem ein Sitzungsschlüssel (K) zwischen einer ersten Computereinheit (U) und einer zweiten Computereinheit (N) vereinbart werden kann, ohne daß ein unbefugter Dritter nützliche Information bezüglich der Schlüssel oder der Identität der ersten Computereinheit (U) erhalten kann. Dies wird erreicht durch die Einbettung des Prinzips des E1-Gamal Schlüsselaustauschs in das erfindungsgemäße Verfahren mit einer zusätzlichen Bildung einer digitalen Unterschrift über einen Hash-Wert des von der ersten Computereinheit (U) gebildeten Sitzungsschlüssels (K).



LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AM	Armenien	GB	Vereinigtes Königreich	MX	Mexiko
AT	Österreich	GE	Georgien	NE	Niger
AU	Australien	GN	Guinea	NL	Niederlande
BB	Barbados	GR	Griechenland	NO	Norwegen
BE	Belgien	HU	Ungarn	NZ	Neuseeland
BF	Burkina Faso	IE	Irland	PL	Polen
BG	Bulgarien	IT	Italien	PT	Portugal
BJ	Benin	JP	Japan	RO	Rumänien
BR	Brasilien	KE	Kenya	RU	Russische Föderation
BY	Belarus	KG	Kirgisistan	SD	Sudan
CA	Kanada	KP	Demokratische Volksrepublik Korea	SE	Schweden
CF	Zentrale Afrikanische Republik	KR	Republik Korea	SG	Singapur
CG	Kongo	KZ	Kasachstan	SI	Slowenien
CH	Schweiz	LI	Liechtenstein	SK	Slowakei
CI	Côte d'Ivoire	LK	Sri Lanka	SN	Senegal
CM	Kamerun	LR	Liberia	SZ	Swasiland
CN	China	LK	Litauen	TD	Tschad
CS	Tschechoslowakei	LU	Luxemburg	TG	Togo
CZ	Tschechische Republik	LV	Lettland	TJ	Tadschikistan
DE	Deutschland	MC	Monaco	TT	Trinidad und Tobago
DK	Dänemark	MD	Republik Moldau	UA	Ukraine
EE	Estland	MG	Madagaskar	UG	Uganda
ES	Spanien	ML	Mali	US	Vereinigte Staaten von Amerika
FI	Finnland	MN	Mongolei	UZ	Usbekistan
FR	Frankreich	MR	Mauretanien	VN	Vietnam
GA	Gabon	MW	Malawi		

Beschreibung

Verfahren zum rechnergestützten Austausch kryptographischer Schlüssel zwischen einer ersten Computereinheit und einer zweiten Computereinheit

Informationstechnische Systeme unterliegen verschiedenen Bedrohungen. So kann z. B. übertragene Information von einem unbefugten Dritten abgehört und verändert werden. Eine weitere Bedrohung bei der Kommunikation zweier Kommunikationspartner liegt in der Vorspiegelung einer falschen Identität eines Kommunikationspartners.

Diesen und weiteren Bedrohungen wird durch verschiedene Sicherheitsmechanismen, die das informationstechnische System vor den Bedrohungen schützen sollen, begegnet. Ein zur Sicherung verwendeter Sicherheitsmechanismus ist die Verschlüsselung der übertragenen Daten. Damit die Daten in einer Kommunikationsbeziehung zwischen zwei Kommunikationspartnern verschlüsselt werden können, müssen vor der Übertragung der eigentlichen Daten zuerst Schritte durchgeführt werden, die die Verschlüsselung vorbereiten. Die Schritte können z. B. darin bestehen, daß sich die beiden Kommunikationspartner auf einen Verschlüsselungsalgorithmus einigen und daß ggf. die gemeinsamen geheimen Schlüssel vereinbart werden.

Besondere Bedeutung gewinnt der Sicherheitsmechanismus der Verschlüsselung bei Mobilfunksystemen, da die übertragenen Daten in diesen Systemen von jedem Dritten ohne besonderen zusätzlichen Aufwand abgehört werden können.

Dies führt zu der Anforderung, eine Auswahl bekannter Sicherheitsmechanismen so zu treffen und diese Sicherheitsmechanis-

men geeignet zu kombinieren, sowie Kommunikationsprotokolle zu spezifizieren, daß durch sie die Sicherheit von informationstechnischen Systemen gewährleistet wird.

Es sind verschiedene asymmetrische Verfahren zum rechnergestützen Austausch kryptographischer Schlüssel bekannt. Asymmetrische Verfahren, die geeignet sind für Mobilfunksysteme, sind (A. Aziz, W. Diffie, "Privacy and Authentication for Wireless Local Area Networks", IEEE Personal Communications, 1994, S. 25 bis 31) und (M. Beller, "Proposed Authentication and Key Agreement Protocol for PCS", Joint Experts Meeting on Privacy and Authentication for Personal Communications, P&A JEM 1993, 1993, S. 1 bis 11).

Das in (A. Aziz, W. Diffie, "Privacy and Authentication in Wireless Local Area Networks", IEEE Personal Communications, 1994, S. 25 bis 31) beschriebene Verfahren bezieht sich ausdrücklich auf lokale Netzwerke und stellt höhere Rechenleistungsanforderungen an die Computereinheiten der Kommunikationspartner während des Schlüsselaustauschs. Außerdem wird in dem Verfahren mehr Übertragungskapazität benötigt als in dem erfindungsgemäßen Verfahren, da die Länge der Nachrichten größer ist als bei dem erfindungsgemäßen Verfahren.

Das in (M. Beller, "Proposed Authentication and Key Agreement Protocol for PCS", Joint Experts Meeting on Privacy and Authentication for Personal Communications, P&A JEM 1993, 1993, S. 1 bis 11) beschriebene Verfahren hat einige grundlegende Sicherheitsziele nicht realisiert. Die explizite Authentifikation des Netzes durch den Benutzer wird nicht erreicht. Außerdem wird ein vom Benutzer an das Netz übertragener Schlüssel vom Netz nicht an den Benutzer bestätigt. Auch eine Zusicherung der Frische (Aktualität) des Schlüssels für das Netz ist nicht vorgesehen. Ein weiterer Nachteil dieses Verfahrens besteht in der Beschränkung auf das Rabin-Verfahren bei der impliziten Authentifizierung des Schlüssels durch den Benutzer. Dies schränkt das Verfahren in einer flexibleren Anwend-

barkeit ein. Außerdem ist kein Sicherheitsmechanismus vorgesehen, der die Nichtabstreitbarkeit von übertragenen Daten gewährleistet. Dies ist ein erheblicher Nachteil vor allem auch bei der Erstellung unanfechtbarer Gebührenabrechnungen für ein Mobilfunksystem. Auch die Beschränkung des Verfahrens auf den National Institute of Standards in Technology Signature Standard (NIST DSS) als verwendete Signaturfunktion schränkt das Verfahren in seiner allgemeinen Verwendbarkeit ein.

Es ist ein Verfahren zum sicheren Datenaustausch zwischen vielen Teilnehmern unter Mitwirkung einer Zertifizierungsinstanz bekannt (US-Patentschrift US 5 214 700). Das bei diesem Verfahren verwendete Protokoll weist eine Zufallszahl, eine Identitätsangabe sowie einen öffentlichen Schlüssel und einen Sitzungsschlüssel auf. Grundlegende Sicherheitsziele werden jedoch bei diesem Verfahren nicht realisiert.

Weiterhin ist ein Verfahren für eine PC-PC-Kommunikation unter Mitwirkung eines Trust-Centers bekannt (DE-Broschüre: Telesec. Telekom, Produktentwicklung Telesec beim Fernmeldeamt Siegen, S. 12-13 und Bild 16).

Aus der US-Patentschrift US 5 222 140 ist ein Verfahren bekannt, bei dem unter Verwendung sowohl eines öffentlichen als auch eines geheimen Schlüssels sowie unter Verwendung einer Zufallszahl ein Sitzungsschlüssel erzeugt wird. Dieser wird mit einem öffentlichen Schlüssel verknüpft.

Weiterhin ist aus der Patentschrift US 5 153 919 ein Verfahren beschrieben, bei dem eine Benutzereinheit sich gegenüber einer Netzeinheit identifiziert. Anschließend findet unter Anwendung einer Hash-Funktion zwischen der Benutzereinheit und der Netzeinheit ein Authentifizierungsprozeß statt.

Weitere sichere Kommunikationsprotokolle, die aber wesentliche grundlegende Sicherheitsziele nicht realisieren, sind be-

kannt (M. Beller et al, Privacy and Authentication on a Portable Communication System, IEEE Journal on Selected Areas in Communications, Vol. 11, No. 6, S. 821-829, 1993).

Das Problem der Erfindung liegt darin, ein vereinfachtes Verfahren zum rechnergestützten Austausch kryptographischer Schlüssel anzugeben.

Dieses Problem wird durch das Verfahren gemäß Patentanspruch 1 gelöst. Vorteilhafte Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

Es wird aus einer ersten Zufallszahl mit Hilfe eines erzeugenden Elements einer endlichen Gruppe in der ersten Computereinheit ein erster Wert gebildet und eine erste Nachricht von der ersten Computereinheit an die zweite Computereinheit übertragen, wobei die ersten Nachricht mindestens den ersten Wert aufweist. In der zweiten Computereinheit wird ein Sitzungsschlüssel mit Hilfe einer ersten Hash-Funktion gebildet, wobei eine erste Eingangsgröße der ersten Hash-Funktion mindestens einen ersten Term aufweist, der gebildet wird durch eine Exponentiation des ersten Werts mit einem geheimen Netzschlüssel. In der ersten Computereinheit wird der Sitzungsschlüssel gebildet mit Hilfe der ersten Hash-Funktion, wobei eine zweite Eingangsgröße der ersten Hash-Funktion mindestens einen zweiten Term aufweist, der gebildet wird durch eine Exponentiation eines öffentlichen Netzschlüssels mit der ersten Zufallszahl. Ferner wird in der ersten Computereinheit mit Hilfe einer zweiten Hash-Funktion oder der ersten Hash-Funktion eine vierte Eingangsgröße gebildet, wobei eine dritte Eingangsgröße für die erste Hash-Funktion oder für die zweite Hash-Funktion zur Bildung der vierten Eingangsgröße mindestens den Sitzungsschlüssel aufweist. Daraufhin wird in der ersten Computereinheit ein Signaturterm aus mindestens der vierten Eingangsgröße gebildet unter Anwendung einer ersten Signaturfunktion. Eine dritte Nachricht wird von der ersten Computereinheit an die zweite Computereinheit übertra-

gen, wobei die dritte Nachricht mindestens den Signaturterm der ersten Computereinheit aufweist. In der zweiten Computereinheit wird der Signaturterm verifiziert.

Die durch das erfindungsgemäße Verfahren erreichten Vorteile liegen vor allem in einer erheblichen Reduktion der Länge der übertragenen Nachrichten und in der Realisierung weiterer Sicherheitsziele.

Durch das erfindungsgemäße Verfahren werden folgende Sicherheitsziele realisiert:

- Gegenseitige explizite Authentifizierung von dem Benutzer und dem Netz, d. h. die gegenseitige Verifizierung der behaupteten Identität,
- Schlüsselvereinbarung zwischen dem Benutzer und dem Netz mit gegenseitiger impliziter Authentifizierung, d. h. daß durch das Verfahren erreicht wird, daß nach Abschluß der Prozedur ein gemeinsamer geheimer Sitzungsschlüssel zur Verfügung steht, von dem jede Partei weiß, daß nur das authentische Gegenüber sich ebenfalls im Besitz des geheimen Sitzungsschlüssels befinden kann,
- Zusicherung der Frische (Aktualität) des Sitzungsschlüssels für den Benutzer,
- gegenseitige Bestätigung des Sitzungsschlüssels von dem Benutzer und dem Netz, d. h. die Bestätigung, daß das Gegenüber tatsächlich im Besitz des vereinbarten geheimen Sitzungsschlüssels ist.

Auf diese Sicherheitsziele beziehen sich auch die folgenden vorteilhaften Weiterbildungen des Verfahrens.

Bei der Weiterbildung des Verfahrens gemäß den Patentanspruch 2 wird zusätzlich in der ersten Computereinheit ein vertrauenswürdiger öffentlicher Benutzerschlüssel der ersten Computereinheit z. B. in Form eines Benutzerzertifikats verfügbar gemacht und in der zweiten Computereinheit wird ein vertrau-

enswürdiger öffentlicher Netzschlüssel der zweiten Computereinheit z. B. in Form eines Netzzertifikats verfügbar gemacht. Der öffentliche Netzschlüssel muß bei dieser Weiterbildung nicht in der ersten Computereinheit verfügbar sein.

Durch die Weiterbildung des Verfahrens gemäß den Patentanspruch 3 ist es nicht nötig, daß der öffentliche Benutzerschlüssel in der zweiten Computereinheit verfügbar ist.

Bei der Weiterbildung des Verfahrens gemäß Patentanspruch 4 ist in der ersten Computereinheit kein vertrauenswürdiger öffentlicher Netzschlüssel der zweiten Computereinheit erforderlich. In der ersten Computerenheit ist ein vertrauenswürdiger öffentlicher Zertifizierungsschlüssel der Zertifizierungscomputereinheit verfügbar. Dies bedeutet, daß die erste Computereinheit sich den vertrauenswürdigen öffentlichen Netzschlüssel in Form eines Netzzertifikats von einer Zertifizierungscomputereinheit "besorgen" muß. Ebenso braucht die zweite Computereinheit den vertrauenswürdigen öffentlichen Benutzerschüssel in Form eines Benutzerzertifikats von der Zertifizierungscomputereinheit.

Durch die Weiterbildungen des erfindungsgemäßen Verfahrens gemäß den Patentansprüchen 6 und 12 wird das Sicherheitsziel der Benutzeranonymität realisiert, d. h. die Vertraulichkeit der Identität des Benutzers gegenüber Dritten.

Die Weiterbildung des erfindungsgemäßen Verfahrens gemäß Patentanspruch 8 ermöglicht die Verwendung von temporären Benutzeridentitäten.

Durch die Weiterbildung des Verfahrens gemäß Patentanspruch 9 wird vor allem eine zusätzliche Authentifizierung der zweiten Computereinheit gegenüber der ersten Computereinheit gewährleistet.

Durch die Weiterbildung gemäß Patentanspruch 11 wird das Sicherheitsziel der Zusicherung der Frische (Aktualität) des Sitzungsschlüssels für das Netz realisiert.

Durch die Weiterbildung des erfindungsgemäßen Verfahrens gemäß Patentanspruch 14 wird zusätzlich das Sicherheitsziel der Nichtabstreitbarkeit von Daten realisiert, die vom Benutzer an das Netz gesendet wurden.

Das erfindungsgemäße Verfahren ist außerdem sehr leicht an unterschiedliche Anforderungen anpaßbar, da es sich nicht auf bestimmte Algorithmen für Signaturbildung und Verschlüsselung beschränkt.

Die Zeichnungen stellen bevorzugte Ausführungsbeispiele der Erfindung dar, die im folgenden näher beschrieben werden.

Es zeigen

Figur 1 ein Ablaufdiagramm, das ein erstes Ausführungsbeispiel des erfindungsgemäßen Verfahrens mit einigen Weiterbildungen darstellt;

Figur 2 ein Ablaufdiagramm, das das erste Ausführungsbeispiel des erfindungsgemäßen Verfahrens mit zusätzlich realisierten Sicherheitszielen mit einigen Weiterbildungen beschreibt.

Figur 3 ein Ablaufdiagramm, das ein zweites Ausführungsbeispiel des erfindungsgemäßen Verfahrens mit einigen Weiterbildungen darstellt;

Figur 4 ein Ablaufdiagramm, das das zweite Ausführungsbeispiel des erfindungsgemäßen Verfahrens mit zusätzlich realisierten Sicherheitszielen mit einigen Weiterbildungen beschreibt.

Figuren 5a, b ein Ablaufdiagramm, das ein drittes Ausführungsbeispiel des erfindungsgemäßen Verfahrens mit einigen Weiterbildungen darstellt;

Figuren 6a, b ein Ablaufdiagramm, das das dritte Ausführungsbeispiel des erfindungsgemäßen Verfahrens mit zusätzlich realisierten Sicherheitszielen mit einigen Weiterbildungen beschreibt.

Erstes Ausführungsbeispiel

In den Figuren 1 und 2 sind durch zwei Skizzen der Ablauf des erfindungsgemäßen Verfahrens dargestellt. Das erfindungsgemäße Verfahren betrifft den Austausch kryptographischer Schlüssel zwischen einer ersten Computereinheit U und einer zweiten Computereinheit N, wobei unter der ersten Computereinheit U eine Computereinheit eines Benutzers eines Mobilfunknetzes zu verstehen ist und unter einer zweiten Computereinheit N eine Computereinheit des Netzbetreibers eines Mobilfunksystems zu verstehen ist.

Die Erfindung beschränkt sich jedoch nicht auf ein Mobilfunksystem und somit auch nicht auf einen Benutzer eines Mobilfunksystems und das Netz, sondern kann in allen Bereichen angewendet werden, in denen ein kryptographischer Schlüsselaustausch zwischen zwei Kommunikationspartnern benötigt wird. Dies kann z. B. in einer Kommunikationsbeziehung zwischen zwei Rechnern, die Daten in verschlüsselter Form austauschen wollen, der Fall sein. Ohne Beschränkung der Allgemeingültigkeit wird im folgenden also ein erster Kommunikationspartner als erste Computereinheit U und ein zweiter Kommunikationspartner als zweite Computereinheit N bezeichnet.

Für das erfindungsgemäße Verfahren gemäß Anspruch 1 wird vorausgesetzt, daß in der ersten Computereinheit U ein vertrauenswürdiger öffentlicher Netzschlüssel g^S der zweiten Computereinheit N verfügbar ist und daß in der zweiten Computereinheit N ein vertrauenswürdiger öffentlicher Benutzer-

schlüssel g^u der ersten Computereinheit U verfügbar ist, wobei g ein erzeugendes Element einer endlichen Gruppe ist.

In der ersten Computereinheit U wird eine erste Zufallszahl t generiert. Aus der ersten Zufallszahl t wird mit Hilfe des erzeugenden Elements g einer endlichen Gruppe in der ersten Computereinheit U ein erster Wert g^t gebildet.

Asymmetrische Verfahren beruhen im wesentlichen auf zwei Problemen der Komplexitätstheorie, dem Problem zusammengesetzte Zahlen effizient zu faktorisieren, und dem diskreten Logarithmusproblem (DLP). Das DLP besteht darin, daß in geeigneten Rechenstrukturen zwar Exponentiationen effizient durchgeführt werden können, daß jedoch für die Umkehrung dieser Operation, das Logarithmieren, keine effizienten Algorithmen bekannt sind.

Solche Rechenstrukturen sind z. B. unter den oben bezeichneten endlichen Gruppen zu verstehen. Diese sind z. B. die multiplikative Gruppe eines endlichen Körpers (z. B. Multiplizieren Modulo p, wobei p eine große Primzahl ist), oder auch sogenannte "elliptische Kurven". Elliptische Kurven sind vor allem deshalb interessant, weil sie bei gleichem Sicherheitsniveau wesentliche kürzere Sicherheitsparameter erlauben. Dies betrifft die Länge der öffentlichen Schlüssel, die Länge der Zertifikate, die Länge der bei der Sitzungsschlüsselvereinbarung auszutauschenden Nachrichten sowie die Länge von digitalen Signaturen, die jeweils im weiteren beschrieben werden. Der Grund dafür ist, daß die für elliptische Kurven bekannten Logarithmierverfahren wesentlich weniger effizient sind als die für endliche Körper.

Eine große Primzahl in diesem Zusammenhang bedeutet, daß die Größe der Primzahl so gewählt werden muß, daß die Logarithmierung so aufwendig ist, daß sie nicht in vertretbarer Zeit durchgeführt werden kann. Vertretbar bedeutet in diesem Zu-

sammenhang einen Zeitraum entsprechend der Sicherheitspolitik von mehreren Jahren bis Jahrzehnten und länger.

Nach der Berechnung des ersten Werts g^t wird eine erste Nachricht M1 codiert, die mindestens den ersten Wert g^t aufweist. Die erste Nachricht M1 wird von der ersten Computereinheit U an die zweite Computereinheit N übertragen.

In der zweiten Computereinheit N wird die erste Nachricht M1 decodiert. Die erste Nachricht M1 kann auch über einen unsicheren Kanal, also auch über eine Luftschnittstelle, unverschlüsselt übertragen werden, da die Logarithmierung des ersten Wertes g^t nicht in vertretbarer Zeit durchgeführt werden kann.

Wie in Figur 2 beschrieben, kann es vorgesehen sein, daß in der zweiten Computereinheit N eine zweite Zufallszahl r generiert wird. Durch diesen zusätzlichen Verfahrensschritt wird ein zusätzliches Sicherheitsziel realisiert: die Zusicherung der Frische (Aktualität) eines im folgenden beschriebenen Sitzungsschlüssels K für die zweite Computereinheit N.

In der zweiten Computereinheit N wird mit Hilfe einer ersten Hash-Funktion h1 ein Sitzungsschlüssel K gebildet. Als eine erste Eingangsgröße der ersten Hash-Funktion h1 wird mindestens ein erster Term verwendet. Der erste Term wird gebildet, indem der erste Wert g^t potenziert wird mit einem geheimen Netzschlüssel s.

Unter einer Hash-Funktion ist in diesem Zusammenhang eine Funktion zu verstehen, bei der es nicht möglich ist, zu einem gegebenen Funktionswert einen passenden Eingangswert zu berechnen. Ferner wird einer beliebig langen Eingangszeichenfolge eine Ausgangszeichenfolge fester Länge zugeordnet. Des weiteren wird für die Hash-Funktion in diesem Zusammenhang Kollisionsfreiheit gefordert, d. h. es darf nicht möglich

sein, zwei verschiedene Eingangszeichenfolgen zu finden, die dieselbe Ausgangszeichenfolge ergeben.

Wenn die zweite Zufallszahl r verwendet wird, so weist die erste Eingangsgröße der ersten Hash-Funktion h1 zusätzlich mindestens die zweite Zufallszahl r auf.

Nun wird in der zweiten Computereinheit N eine Antwort A gebildet. Zur Bildung der Antwort A sind verschiedene Varianten vorgesehen. So ist es z. B. möglich, daß mit dem Sitzungsschlüssel K unter Verwendung einer Verschlüsselungsfunktion Enc eine Konstante const verschlüsselt wird. Die Konstante const ist sowohl der ersten Computereinheit U als auch der zweiten Computereinheit N bekannt. Auch die Verschlüsselungsfunktion Enc ist sowohl der zweiten Computereinheit N als auch der ersten Computereinheit U als die in dem Verfahren zu verwendende Verschlüsselungsfunktion bekannt.

Eine weitere Möglichkeit, die Antwort A zu bilden liegt z. B. darin, daß der Sitzungsschlüssel K als Eingangsgröße für eine dritte Hash-Funktion h3 verwendet wird und der "gehashte" Wert des Sitzungsschlüssels K als Antwort A verwendet wird. Weitere Möglichkeiten, die Antwort A zu bilden, die zur Überprüfung des Sitzungsschlüssels K in der ersten Computereinheit U verwendet wird, sind dem Fachmann geläufig und können als Varianten zu den beschriebenen Vorgehensweisen verwendet werden.

Eine Aneinanderreihung der zweiten Zufallszahl r, der Antwort A, sowie ein optionales erstes Datenfeld dat1 bilden eine zweite Nachricht M2. Die zweite Zufallszahl r und das optionale erste Datenfeld dat1 sind nur in der zweiten Nachrichten 112 enthalten, wenn diese in dem erfindungsgemäßen Verfahren vorgesehen werden.

Die zweite Nachricht M2 wird in der zweiten Computereinheit N codiert und zu der ersten Computereinheit U übertragen.

In der ersten Computereinheit U wird die zweite Nachricht M2 decodiert, so daß die erste Computereinheit U eventuell die zweite Zufallszahl r, die Antwort A sowie eventuell das optionale erste Datenfeld dat1 zur Verfügung hat. Die Länge des optionalen ersten Datenfeldes dat1 kann beliebig groß sein, d. h. es ist auch möglich, daß das optionale erste Datenfeld dat1 nicht vorhanden ist.

In der ersten Computereinheit U wird nun ebenfalls der Sitzungsschlüssel K gebildet, mit Hilfe der ersten Hash-Funktion h1, die sowohl der zweiten Computereinheit N als auch der ersten Computereinheit U bekannt ist. Eine zweite Eingangsgröße der ersten Hash-Funktion h1 zur Bildung des Sitzungsschlüssels K in der ersten Computereinheit U weist mindestens einen zweiten Term auf. Der zweite Term wird gebildet aus einer Exponentation eines öffentlichen Netzschlüssels g^s mit der ersten Zufallszahl t. Wenn die Verwendung der zweiten Zufallszahl r in dem erfindungsgemäßen Verfahren vorgesehen wird, so weist die zweite Eingangsgröße der ersten Hash-Funktion h1 zur Bildung des Sitzungsschlüssels K in der ersten Computereinheit U zusätzlich die zweite Zufallszahl auf.

Durch die Verwendung der ersten Zufallszahl t und der zweiten Zufallszahl r bei der Generierung des Sitzungsschlüssels K wird die Aktualität des Sitzungsschlüssels K gewährleistet, da jeweils die erste Zufallszahl t als auch die zweite Zufallszahl r nur für jeweils einen Sitzungsschlüssel K verwendet werden.

Somit wird eine Wiedereinspielung eines älteren Schlüssels als Sitzungsschlüssel K verhindert. Die Aktualität des Sitzungsschlüssels K ist auch bedeutend im Zusammenhang mit der Fragestellung, wie groß die erste Zufallszahl t sowie die zweite Zufallszahl r sein müssen. Dies wird deutlich, da eine geringere Länge der Zufallszahlen das DLP-Problem verringern, d. h. je kürzer die Zufallszahl ist, desto einfacher ist die

Logarithmierung, also z. B. das Herausfinden der ersten Zufallszahl t aus dem ersten Wert g^t. Wenn aber für jeden neuen Sitzungsschlüssel K andere Zufallszahlen verwendet werden, so ist die Wahrscheinlichkeit, daß der verwendete Sitzungsschlüssel K von einem unbefugten Dritten schon herausgefunden wurde, wesentlich geringer. Damit ist die Gefahr, daß der Teil einer Nachricht, der mit dem Sitzungsschlüssel K verschlüsselt ist, von einem unbefugten Dritten entschlüsselt werden kann, erheblich reduziert.

Nachdem in der ersten Computereinheit U der Sitzungsschlüssel K gebildet wurde, wird anhand der empfangenen Antwort A überprüft, ob der in der ersten Computereinheit U gebildete Sitzungsschlüssel K mit dem Sitzungsschlüssel K, der in der zweiten Computereinheit N gebildet wurde, übereinstimmt. Abhängig von den im vorigen beschriebenen Varianten zur Bildung der Antwort A sind verschiedene Möglichkeiten vorgesehen, den Sitzungsschlüssel K anhand der Antwort A zu überprüfen.

Eine Möglichkeit besteht z. B. darin, daß, wenn die Antwort A in der zweiten Computereinheit N durch Verschlüsselung der Konstante const mit dem Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc gebildet wurde, die Antwort A entschlüsselt wird, und somit die erste Computereinheit U eine entschlüsselte Konstante const' erhält, die mit der bekannten Konstante const verglichen wird.

Die Überprüfung des Sitzungsschlüssels K anhand der Antwort A kann auch durchgeführt werden, indem die der ersten Computereinheit U bekannte Konstante const mit dem in der ersten Computereinheit U gebildeten Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc verschlüsselt wird und das Ergebnis mit der Antwort A auf Übereinstimmung geprüft wird. Diese Vorgehensweise wird z. B. auch verwendet, wenn die Antwort A in der zweiten Computereinheit N gebildet wird, indem auf den Sitzungsschlüssel K die dritte Hash-Funktion h3 angewendet wird. In diesem Fall wird in der ersten

Computereinheit U der in der ersten Computereinheit U gebildete Sitzungsschlüssel K als Eingangsgröße der dritten Hash-Funktion h3 verwendet. Der "gehashte" Wert des in der ersten Computereinheit U gebildeten Sitzungsschlüssels K wird dann mit der Antwort A auf Übereinstimmung geprüft. Damit wird das Ziel der Schlüsselbestätigung des Sitzungsschlüssels K erreicht.

Dadurch, daß bei der Berechnung des Sitzungsschlüssels K in der zweiten Computereinheit N der geheime Netzschlüssel s und bei der Berechnung des Sitzungsschlüssels K in der ersten Computereinheit U der öffentliche Netzschlüssel g^s verwendet werden, wird die zweite Computereinheit N durch die erste Computereinheit U authentifiziert. Dies wird erreicht, vorausgesetzt daß für die erste Computereinheit U bekannt ist, daß der öffentliche Netzschlüssel g^s tatsächlich zur zweite Computereinheit N gehört.

Im Anschluß an die Bestätigung des Sitzungsschlüssels K durch Überprüfung der Antwort A wird ein Signaturterm berechnet. Hierzu wird mit Hilfe einer zweiten Hash-Funktion h2 eine vierte Eingangsgröße gebildet. Die zweite Hash-Funktion h2 kann, muß aber nicht dieselbe Hash-Funktion sein wie die erste Hash-Funktion h1. Als eine dritte Eingangsgröße für die zweite Hash-Funktion h2 wird ein Term verwendet, der mindestens den Sitzungsschlüssel K enthält. Weiterhin kann die dritte Eingangsgröße das optionale erste Datenfeld dat1 oder auch ein optionales zweites Datenfeld dat2 enthalten, wenn deren Verwendung in dem erfindungsgemäßen Verfahren vorgesehen wird.

Es kann später nicht abgestritten werden, daß die Daten, die im ersten optionale Datenfeld dat1 und im zweiten optionalen Datenfeld dat2 enthalten sind, von der ersten Computereinheit U gesendet wurden.

Die in dem ersten optionalen Datenfeld dat1 und in dem zweiten optionalen Datenfeld dat2 enthaltenen Daten können z. B. Telefonnummern, die aktuelle Zeit oder ähnliche hierfür geeignete Parameter sein. Diese Information kann als Werkzeug für eine unanfechtbare Gebührenabrechnung verwendet werden.

Unter Verwendung einer ersten Signaturfunktion Sig_U wird der Signaturterm aus mindestens der vierten Eingangsgröße gebildet. Um einen höheren Sicherheitsgrad zu erzielen, kann der Signaturterm verschlüsselt werden. Der Signaturterm wird in diesem Fall mit dem Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc verschlüsselt und bildet den ersten verschlüsselten Term VT1.

Außerdem wird, falls das Sicherheitsziel "Anonymität des Benutzers" realisiert werden soll, ein zweiter verschlüsselter Term VT2 berechnet, in dem eine Identitätsgröße IMUI der ersten Computereinheit U mit dem Sitzungschlüssel K mit Hilfe der Verschlüsselungsfunktion Enc verschlüsselt wird. Bei Verwendung eines optionalen zweiten Datenfeldes dat2 wird in der ersten Computereinheit U ein dritter verschlüsselter Term VT3 berechnet, indem das optionale zweite Datenfeld dat2 mit dem Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc verschlüsselt wird, das optionale zweite Datenfeld dat2 kann auch unverschlüsselt übertragen werden.

In der ersten Computereinheit U wird eine dritte Nachricht M3 gebildet und codiert, die mindestens den Signaturterm und die Identitätsgröße IMUI der ersten Computereinheit U aufweist.

Falls die Anonymität der ersten Computereinheit U gewährleistet werden soll, weist die dritte Nachricht M3 anstatt der Identitäsgröße IMUI der ersten Computereinheit U mindestens den zweiten verschlüsselten Term VT2 auf, der die Information über die Identität der ersten Computereinheit U in ver-

schlüsselter Form enthält, die nur von der zweiten Computereinheit N entschlüsselt werden kann.

Wenn die Verwendung des optionalen zweiten Datenfelds dat2 vorgesehen wird, weist die dritte Nachricht M3 zusätzlich mindestens den dritten verschlüsselten Term VT3 oder das optionale zweite Datenfeld dat2 im Klartext auf.

Wenn die dritte Nachricht M3 den ersten verschlüsselten Term VT1, den zweiten verschlüsselten Term VT2 oder den dritten verschlüsselten Term VT3 enthält, werden diese in der zweiten Computereinheit N entschlüsselt. Dies geschieht für den eventuell vorhandenen ersten verschlüsselten Term VT1 vor der Verifikation des Signaturterms.

Die dritte Nachricht M3 wird von der ersten Computereinheit U zu der zweiten Computereinheit N übertragen.

Zusätzlich wird die Authentifikation der ersten Computereinheit U gegenüber der zweiten Computereinheit N durch den Signaturterm gewährleistet, durch deren Verwendung garantiert wird, daß die dritte Nachricht M3 tatsächlich aktuell von der ersten Computereinheit U gesendet wurde.

In der zweiten Computereinheit N wird die dritte Nachricht M3 decodiert und anschließend wird anhand eines Benuterzertifikats CertU, das der zweiten Computereinheit N zur Verfügung steht, der Signaturterm verifiziert.

Wenn für das erfindungsgemäße Verfahren temporäre Benutzeridentitäten vorgesehen werden, so wird das im vorigen beschriebene Verfahren um einige Verfahrensschritte erweitert.

Zuerst muß der zweiten Computereinheit N bekannt gemacht werden, welche erste Computereinheit U eine neue temporäre Identitätsgröße TMUIN von der zweiten Computereinheit N zugewiesen bekommen soll.

Hierzu wird als zusätzlicher Bestandteil der ersten Nachricht M1 eine alte temporäre Identitätsgröße TMUIO von der ersten Computereinheit U an die zweite Computereinheit N übertragen.

Nach Empfang der ersten Nachricht M1 ist somit in der zweiten Computereinheit N bekannt, für welche erste Computereinheit U die neue temporäre Identitätsgröße TMUIN bestimmt ist.

In der zweiten Computereinheit N wird dann die neue temporäre Identitätsgröße TMUIN für die erste Computereinheit U gebildet. Dies kann z. B. durch Generierung einer Zufallszahl oder durch Tabellen, in denen mögliche Identitätsgrößen abgespeichert sind, durchgeführt werden. Aus der neuen temporären Identitätsgröße TMUIN der ersten Computereinheit U wird in der zweiten Computereinheit N ein vierter verschlüsselter Term VT4 gebildet, indem die neue temporäre Identitätsgröße TMUIN der ersten Computereinheit U mit dem Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc verschlüsselt wird.

In diesem Fall weist die zweite Nachricht N2 zusätzlich mindestens den vierten verschlüsselten Term VT4 auf. Der vierte verschlüsselte Term VT4 wird dann in der ersten Computereinheit U entschlüsselt. Nun ist die neue temporäre Identitätsgörße TMUIN der ersten Computereinheit U in der ersten Computereinheit U verfügbar.

Damit der zweiten Computereinheit N auch gewährleistet wird, daß die erste Computereinheit U die neue temporäre Identitätsgröße TMUIN korekt empfangen hat, weist die dritte Eingangsgröße für die erste Hash-Funktion h1 oder für die zweite Hash-Funktion h2 zusätzlich mindestens die neue temporäre Identitätsgröße TMUIN der ersten Computereinheit U auf.

Da die Information der neuen temporären Identitätsgröße TMUIN in dem Signaturterm in diesem Fall enthalten ist, weist die

dritte Nachricht M3 nicht mehr die Identitätsgröße IMUI der ersten Computereinheit U auf.

Es ist auch möglich, die neue temporäre Identitätsgröße TMUIN nicht in den Signaturterm zu integrieren, sondern den zweiten verschlüsselten Term VT2 zu bilden, indem anstant der Identitätsgröße IMUI der ersten Computereinheit U die neue temporäre Identitätsgröße TMUIN mit dem Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc verschlüsselt wird. In diesem Fall weist die dritte Nachricht M3 zusätzlich den zweiten verschlüsselten Term VT2 auf.

Die in dem erfindungsgemäßen Verfahren verwendeten Hash-Funktionen, die erste Hash-Funktion h1, die zweite Hash-Funktion h2 und die dritte Hash-Funktion h3 können durch die gleiche, aber auch durch verschiedene Hash-Funktionen realisiert werden.

Zweites Ausführungsbeispiel

In den Figuren 3 und 4 sind durch zwei Skizzen der Ablauf eines zweiten Ausführungsbeispiels des erfindungsgemäßen Verfahrens dargestellt.

Für dieses Ausführungsbeispiel des Verfahrens wird vorausgesetzt, daß in der ersten Computereinheit U ein vertrauenswürdiger öffentlicher Benutzerschlüssel g^u der ersten Computereinheit U z. B. in Form eines Benutzerzertifikats CertU verfügbar gemacht wird und daß in der zweiten Computereinheit N ein vertrauenswürdiger öffentlicher Netzschlüssel g^s der zweiten Computereinheit N z. B. in Form eines Netzzertifikats CertN verfügbar gemacht wird. Der öffentliche Netzschlüssel g^s muß nicht in der ersten Computereinheit U verfügbar sein. Ebenso ist es nicht nötig, daß der öffentliche Benutzerschlüssel g^u in der zweiten Computereinheit N verfügbar ist.

In der ersten Computereinheit U wird eine erste Zufallszahl t generiert. Aus der ersten Zufallszahl t wird mit Hilfe des erzeugenden Elements g einer endlichen Gruppe in der ersten Computereinheit U ein erster Wert g^t gebildet.

Nach der Berechnung des ersten Werts g^t wird eine erste Nachricht M1 codiert, die mindestens den ersten Wert g^t und eine Identitätsangabe id_{CA} einer Zertifizierungscomputereinheit CA, die das Netzzertifikat CertN liefert, das von der ersten Computereinheit U verifiziert werden kann, aufweist. Die erste Nachricht M1 wird von der ersten Computereinheit U an die zweite Computereinheit N übertragen.

In der zweiten Computereinheit N wird die erste Nachricht M1 decodiert. Die erste Nachricht M1 kann auch über einen unsicheren Kanal, also auch über eine Luftschnittstelle, unverschlüsselt übertragen werden, da die Logarithmierung des ersten Wertes g^t nicht in vertretbarer Zeit durchgeführt werden kann.

Wie in Figur 4 beschrieben, kann es vorgesehen sein, daß in der zweiten Computereinheit N eine zweite Zufallszahl r generiert wird. Durch diesen zusätzlichen Verfahrensschritt wird ein zusätzliches Sicherheitsziel realisiert: die Zusicherung der Frische (Aktualität) eines im folgenden beschriebenen Sitzungsschlüssels K für die zweite Computereinheit N.

In der zweiten Computereinheit N wird mit Hilfe einer ersten Hash-Funktion h1 ein Sitzungsschlüssel K gebildet. Als eine erste Eingangsgröße der ersten Hash-Funktion h1 wird ein erster Term verwendet. Der erste Term wird gebildet, indem der erste Wert g^t potenziert wird mit einem geheimen Netzschlüssel s.

Wenn die zweite Zufallszahl r verwendet wird, so weist die erste Eingangsgröße der ersten Hash-Funktion h1 zusätzlich mindestens die zweite Zufallszahl r auf. Nun wird in der

zweiten Computereinheit N eine Antwort A gebildet. Zur Bildung der Antwort A sind verschiedene Varianten vorgesehen. Es ist z. B. möglich, daß mit dem Sitzungsschlüssel K unter Verwendung einer Verschlüsselungsfunktion Enc eine Konstante const verschlüsselt wird. Die Konstante const ist sowohl der ersten Computereinheit U als auch der zweiten Computereinheit N bekannt. Auch die Verschlüsselungsfunktion Enc ist sowohl der zweiten Computereinheit N als auch der ersten Computereinheit U als die in dem erfindungsgemäßen Verfahren zu verwendende Verschlüsselungsfunktion bekannt.

Eine weitere Möglichkeit, die Antwort A zu bilden liegt z. B. darin, daß der Sitzungsschlüssel K als Eingangsgröße für eine dritte Hash-Funktion h 3 verwendet wird und der "gehashte" Wert des Sitzungsschlüssels K als Antwort verwendet wird. Weitere Möglichkeiten, die Antwort A zu bilden, die zur Überprüfung des Sitzungsschlüssels K in der ersten Computereinheit U verwendet wird, sind dem Fachmann geläufig und können als Varianten zu den beschriebenen Vorgehensweisen verwendet werden.

Eine Aneinanderreihung der zweiten Zufallszahl r, des Netzzertifikats CertN, der Antwort A, sowie ein optionales erstes Datenfeld dat1 bilden eine zweite Nachricht M2. Die zweite Zufallszahl r und das optionale erste Datenfeld dat1 sind nur in der zweiten Nachricht M2 enthalten, wenn diese in dem erfindungsgemäßen Verfahren vorgesehen sind.

Die zweite Nachricht M2 wird in der zweiten Computereinheit N codiert und zu der ersten Computereinheit U übertragen.

In der ersten Computereinheit U wird die zweite Nachricht M2 decodiert, so daß die erste Computereinheit U eventuell die zweite Zufallszahl r, die Antwort A sowie eventuell das optionale erste Datenfeld dat1 zur Verfügung hat. Die Länge des optionalen ersten Datenfeldes dat1 kann beliebig groß sein,

d. h. es ist auch möglich, daß das optionale erste Datenfeld dat1 nicht vorhanden ist.

Anschließend wird das in der zweiten Nachricht M2 enthaltene Netzzertifikat CertN in der ersten Computereinheit verifiziert. Somit steht der öffentliche Netzschlüssel g^S in der ersten Computereinheit U zur Verfügung.

In der ersten Computereinheit U wird nun ebenfalls der Sitzungsschlüssel K gebildet, mit Hilfe der ersten Hash-Funktion h1, die sowohl in der zweiten Computereinheit N als auch in der ersten Computereinheit U bekannt ist. Eine zweite Eingangsgröße der ersten Hash-Funktion h1 zur Bildung des Sitzungsschlüssels K in der ersten Computereinheit U weist mindestens einen zweiten Term auf. Der zweite Term wird gebildet aus einer Exponentation eines öffentlichen Netzschlüssels g^S mit der ersten Zufallszahl t. Wenn die Verwendung der zweiten Zufallszahl r in dem erfindungsgemäßen Verfahren vorgesehen wird, so weist die zweite Eingangsgröße der ersten Hash-Funktion h1 zur Bildung des Sitzungsschlüssels K in der ersten Computereinheit U zusätzlich die zweite Zufallszahl r auf.

Durch die Verwendung der ersten Zufallszahl t und der zweiten Zufallszahl r bei der Generierung des Sitzungsschlüssels K wird die Aktualität des Sitzungsschlüssels K gewährleistet, da jeweils die erste Zufallszahl t als auch die zweite Zufallszahl r nur für jeweils einen Sitzungsschlüssel K verwendet werden.

Somit wird eine Wiedereinspielung eines älteren Schlüssels als Sitzungsschlüssel K verhindert. Die Aktualität des Sitzungsschlüssels K ist auch bedeutend im Zusammenhang mit der Fragestellung, wie groß die erste Zufallszahl t sowie die zweite Zufallszahl r sein müssen. Dies wird deutlich, da eine geringere Länge der Zufallszahlen das DLP-Problem verringern, d. h. je kürzer die Zufallszahl ist, desto einfacher ist die

Logarithmierung, also z. B. das Herausfinden der ersten Zufallszahl t aus dem ersten Wert g^t. Wenn aber für jeden neuen Sitzungsschlüssel K andere Zufallszahlen verwendet werden, so ist die Wahrscheinlichkeit, daß der verwendete Sitzungsschlüssel K von einem unbefugten Dritten schon herausgefunden wurde, wesentlich geringer. Damit ist die Gefahr, daß der Teil einer Nachricht, der mit dem Sitzungsschlüssel K verschlüsselt ist, von einem unbefugten Dritten entschlüsselt werden kann, erheblich reduziert.

Nachdem in der ersten Computereinheit U der Sitzungsschlüssel K gebildet wurde, wird anhand der empfangenen Antwort A überprüft, ob der in der ersten Computereinheit U gebildete Sitzungsschlüssel K mit dem Sitzungsschlüssel K, der in der zweiten Computereinheit N gebildet wurde, übereinstimmt.

Abhängig von den im vorigen beschriebenen Varianten zur Bildung der Antwort A sind verschiedene Möglichkeiten vorgesehen, den Sitzungsschlüssel K anhand der Antwort A zu überprüfen.

Eine Möglichkeit besteht z. B. darin, daß, wenn die Antwort A in der zweiten Computereinheit N durch Verschlüsselung der Konstante const mit dem Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc gebildet wurde, die Antwort A entschlüsselt wird, und somit die erste Computereinheit U eine entschlüsselte Konstante const' erhält, die mit der bekannten Konstante const verglichen wird.

Die Überprüfung des Sitzungsschlüssels K anhand der Antwort A kann auch durchgeführt werden, indem die der ersten Computereinheit U bekannte Konstante const mit dem in der ersten Computereinheit U gebildeten Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc verschlüsselt wird und das Ergebnis mit der Antwort A auf Übereinstimmung geprüft wird. Diese Vorgehensweise wird z. B. auch verwendet, wenn die Antwort A in der zweiten Computereinheit N gebildet

wird, in dem auf den Sitzungsschlüssel K die dritte Hash-Funktion h3 angewendet wird. In diesem Fall wird in der ersten Computereinheit U der in der ersten Computereinheit U gebildete Sitzungsschlüssel K als Eingangsgröße der dritten Hash-Funktion h3 verwendet. Der "gehashte" Wert des in der ersten Computereinheit U gebildeten Sitzungsschlüssels K wird dann mit der Antwort A auf Übereinstimmung geprüft. Damit wird das Ziel der Schlüsselbestätigung des Sitzungsschlüssels K erreicht.

Dadurch, daß bei der Berechnung des Sitzungsschlüssels K in der zweiten Computereinheit N der geheime Netzschlüssel s und bei der Berechnung des Sitzungsschlüssels K in der ersten Computereinheit U der öffentliche Netzschlüssel g^s verwendet werden, wird die zweite Computereinheit N durch die erste Computereinheit U authentifiziert. Dies wird erreicht, vorausgesetzt daß für die erste Computereinheit U bekannt ist, daß der öffentliche Netzschlüssel g^s tatsächlich zur zweiten Computereinheit N gehört.

Im Anschluß an die Bestätigung des Sitzungsschlüssels K durch Überprüfung der Antwort A wird ein Signaturterm berechnet. Hierzu wird mit Hilfe einer zweiten Hash-Funktion h2 eine vierte Eingangsgröße gebildet. Die zweite Hash-Funktion h2 kann, muß aber nicht dieselbe Hash-Funktion sein wie die erste Hash-Funktion h1. Als eine dritte Eingangsgröße für die zweite Hash-Funktion h2 wird ein Term verwendet, der mindestens den Sitzungsschlüssel K enthält. Weiterhin kann die dritte Eingangsgröße das optionale erste Datenfeld dat1 oder auch ein optionales zweites Datenfeld dat2 enthalten, wenn deren Verwendung in dem erfindungsgemäßen Verfahren vorgesehen wird.

Es kann später nicht abgestritten werden, daß die Daten, die im ersten optionale Datenfeld dat1 und im zweiten optionalen Datenfeld dat2 enthalten sind, von der ersten Computereinheit U gesendet werden.

Die in dem ersten optionalen Datenfeld dat1 und in dem zweiten optionalen Datenfeld dat2 enthaltenen Daten können z. B. Telefonnummern, die aktuelle Zeit oder ähnliche hierfür geeignete Parameter sein. Diese Information kann als Werkzeug für eine unanfechtbare Gebührenabrechnung verwendet werden.

Unter Verwendung einer ersten Signaturfunktion Sig_U wird der Signaturterm aus mindestens der vierten Eingangsgröße gebildet. Um einen höheren Sicherheitsgrad zu erzielen, kann der Signaturterm verschlüsselt werden. Der Signaturterm wird in diesem Fall mit dem Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc verschlüsselt und bildet den ersten verschlüsselten Term VT1.

Außerdem wird, falls das Sicherheitsziel "Anonymität des Benutzers" realisiert werden soll, ein zweiter verschlüsselter Term VT2 berechnet, in dem ein Benutzerzertifikat CertU der ersten Computereinheit U mit dem Sitzungschlüssel K mit Hilfe der Verschlüsselungsfunktion Enc verschlüsselt wird. Bei Verwendung eines optionalen zweiten Datenfeldes dat2 kann in der ersten Computereinheit U ein dritter verschlüsselter Term VT3 berechnet werden, indem das optionale zweite Datenfeld dat2 mit dem Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc verschlüsselt wird. Das optionale zweite Datenfeld dat2 kann ebenso unverschlüselt übertragen werden.

In der ersten Computereinheit U wird eine dritte Nachricht M3 gebildet und codiert, die mindestens den Signaturterm und das Benutzerzertifikat CertU der ersten Computereinheit U aufweist. Falls die Benutzeranonymität der ersten Computereinheit U gewährleistet werden soll, weist die dritte Nachricht M3 anstatt des Benutzerzertifikats CertU der ersten Computereinheit U mindestens den zweiten verschlüsselten Term VT2 auf, der das Benutzerzertifikat CertU der ersten Computereinheit U in verschlüsselter Form enthält, die nur von der zweiten Computereinheit N entschlüsselt werden kann.

Wenn die Verwendung des optionalen zweiten Datenfelds dat2 vorgesehen wird, weist die dritte Nachricht M3 zusätzlich mindestens den dritten verschlüsselten Term VT 3 auf. Wenn die dritte Nachricht M3 den ersten verschlüsselten Term VT1, den zweiten verschlüsselten Term VT2 oder den dritten verschlüsselten Term VT3 aufweist, werden diese in der zweiten Computereinheit N entschlüsselt. Dies geschieht für den eventuell vorhandenen ersten verschlüsselten Term VT1 vor der Verifikation des Signaturterms.

Die dritte Nachricht M3 wird von der ersten Computereinheit U zu der zweiten Computereinheit N übertragen.

Zusätzlich wird die Authentifikation der ersten Computereinheit U gegenüber der zweiten Computereinheit N durch den Signaturterm gewährleistet, durch deren Verwendung garantiert wird, daß die dritte Nachricht M3 tatsächlich aktuell von der ersten Computereinheit U gesendet wurde.

Wenn für das erfindungsgemäße Verfahren temporäre Benutzeridentitäten vorgesehen werden, so wird das im vorigen beschriebene Verfahren um einige Verfahrensschritte erweitert.

In der zweiten Computereinheit N wird für die erste Computereinheit U eine neue temporäre Identitätsgröße TMUIN gebildet, die der ersten Computereinheit U im weiteren zugewiesen wid. Dies kann z. B. durch Generierung einer Zufallszahl oder durch Tabellen, in denen mögliche Identitätsgrößen abgespeichert sind, durchgeführt werden. Aus der neuen temporären Identitätsgröße TMUIN der ersten Computereinheit U wird in der zweiten Computereinheit N ein vierter verschlüsselter Term VT4 gebildet, indem die neue temporäre Identitätsgröße TMUIN der ersten Computereinheit U mit dem Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc verschlüsselt wird.

In diesem Fall weist die zweite Nachricht M2 zusätzlich mindestens den vierten verschlüsselten Term VT4 auf. Der vierte verschlüsselte Term VT4 wird dann in der ersten Computereinheit U entschlüsselt. Nun ist die neue temporäre Identitätsgröße TMUIN der ersten Computereinheit U in der ersten Computereinheit U verfügbar.

Damit der zweiten Computereinheit N auch gewährleistet wird, daß die erste Computereinheit U die neue temporäre Identitätsgröße TMUIN korrekt empfangen hat, weist die dritte Eingangsgröße für die erste Hash-Funktion h1 oder für die zweite Hash-Funktion h2 zusätzlich mindestens die neue temporäre Identitätsgröße TMUIN der ersten Computereinheit U auf.

Es ist auch möglich, die neue temporäre Identitätsgröße TMUIN nicht in den Signaturterm zu integrieren, sondern den zweiten verschlüsselten Term VT2 zu bilden, indem die neue temporäre Identitätsgröße TMUIN der ersten Computereinheit U mit dem Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc verschlüsselt wird. In diesem Fall weist die dritte Nachricht M3 zusätzlich den zweiten verschlüsselten Term VT2 auf.

Drittes Ausführungsbeispiel

In den Figuren 5a, b sind durch zwei Skizzen der Ablauf eines dritten Ausführungsbeispiels dargestellt.

Für diese Weiterbildung des Verfahrens wird vorausgesetzt, daß in der ersten Computereinheit U kein vertrauenswürdiger öffentlicher Netzschlüssel g^s der zweiten Computereinheit N verfügbar ist. In der Benutzercomputerenheit U ist ein vertrauenswürdiger öffentlicher Zertifizierungsschlüssel g^u der Zertifizierungscomputereinheit CA verfügbar, wobei g ein erzeugendes Element einer endlichen Gruppe ist. Dies bedeutet, daß die erste Computereinheit U sich den vertrauenswürdigen öffentlichen Netzschlüssel g^s in Form eines Netzzertifikats

CertN von einer Zertifizierungscomputereinheit CA "besorgen" muß. Ebenso braucht die zweiten Computereinheit N den vertrauenswürdigen öffentlichen Benutzerschüssel g^u in Form eines Benutzerzertifikats CertU von der Zertifizierungscomputereinheit CA.

In der ersten Computereinheit U wird eine erste Zufallszahl t generiert. Aus der ersten Zufallszahl t wird mit Hilfe des erzeugenden Elements g einer endlichen Gruppe in der ersten Computereinheit U ein erster Wert g^t gebildet.

Nach der Berechnung des ersten Werts g^t wird eine erste Nachricht M1 codiert, die mindestens den ersten Wert g^t, eine Identitätsgröße IMUI der ersten Computereinheit U und eine Identitätsgröße id_{CA} einer Zertifizierungscomputereinheit CA, die ein Netzzertifikat CertN liefert, das von der ersten Computereinheit U verifiziert werden kann, aufweist. Dies ist nötig, wenn mehrere Zertifizierungsinstanzen mit unterschiedlichen geheimen Zertifizierungsschlüsseln vorgesehen werden. Wenn das Sicherheitsziel der Benutzeranonymität realisiert werden soll, wird in der ersten Computereinheit U vor Bildung der ersten Nachricht M1 ein Zwischenschlüssel L gebildet. Dies geschieht durch Potenzierung des öffentlichen Zertifizierungsschlüssels g^u mit der ersten Zufallszahl t. Im weiteren wird in diesem Fall die Identitätsgröße IMUI der ersten Computereinheit U mit dem Zwischenschlüssel L unter Anwendung einer Verschlüsselungsfunktion Enc verschlüsselt und das Ergebnis stellt einen vierten verschlüsselten Term VT4 dar. Der vierte verschlüsselte Term VT4 wird anstatt der Identitätsgröße IMUI der ersten Computereinheit U in die erste Nachricht M1 integriert. Die erste Nachricht M1 wird von der ersten Computereinheit U an die zweiten Computereinheit N übertragen.

In der zweiten Computereinheit N wird die erste Nachricht M1 decodiert. Die erste Nachricht M1 kann auch über einen unsicheren Kanal, also auch über eine Luftschnittstelle, unver-

schlüsselt übertragen werden, da die Logarithmierung des ersten Wertes g^t nicht in vertretbarer Zeit durchgeführt werden kann.

In der zweiten Computereinheit N wird die erste Nachricht M1 decodiert, und eine vierte Nachricht M4 gebildet, die eine Verkettung des der zweiten Computereinheit N bekannten öffentlichen Netzschlüssels g^s, dem ersten Wert g^t und der Identitätsgröße IMUI der ersten Computereinheit U, sowie einem ersten signierten Term aufweist. Der erste signierte Term wird gebildet durch Anwendung einer zweiten Signaturfunktion Sig_N auf einen ersten Signatureingangsterm. Der erste Signatureingangsterm weist mindestens ein Ergebnis einer dritten Hash-Funktion h3 auf, die auf mindestens eine Verkettung des öffentlichen Netzschlüssels g^s, des ersten Werts g^t und der Identitätsgröße IMUI der ersten Computereinheit U angewendet wird. In dem Fall, daß das Sicherheitsziel der Benutzeranonymität realisiert werden soll, wird in der vierten Nachricht M4 anstatt der Identitätsgröße IMUI der ersten Computereinheit U der vierte verschlüsselte Term VT4 codiert. In diesem Fall weist auch die Verkettung, auf die die dritte Hash-Funktion h3 angewendet wird, anstatt der Identitätsgröße IMUI der ersten Computereinheit U den vierten verschlüsselten Term VT4 auf.

Die zweite Signaturfunktion Sig_N kann, muß aber nicht gleich sein der ersten Signaturfunktion Sig_U.

Die vierte Nachricht M4 wird in der zweiten Computereinheit N codiert und anschließend an die Zertifizierungscomputereinheit CA übertragen.

In der Zertifizierungscomputereinheit CA wird die vierte Nachricht M4 decodiert und mit dem öffentlichen Schlüssel g^s, der der Zertifizierungscomputereinheit CA bekannt ist, verifiziert. Damit wird die zweiten Computereinheit N als Sender der vierten Nachricht M4 authentifiziert.

Anschließend wird, falls die Benutzeranonymität gewährleistet wird, also der vierte verschlüsselte Term VT4 in der vierten Nachricht M4 mitgesendet wurde, in der Zertifizierungscomputereinheit CA der Zwischenschlüssel L berechnet, indem der erste Wert g^t mit einem geheimen Zertifizierungsschlüssel u der Zertifizierungscomputereinheit CA potenziert wird.

Mit dem Zwischenschlüssel L wird unter Verwendung der Verschlüsselungsfunktion Enc der vierte verschlüsselte Term VT4 entschlüsselt, womit in der Zertifizierungscomputereinheit CA die Identitätsgröße IMUI der ersten Computereinheit U bekannt ist.

In der Zertifizierungscomputereinheit CA wird dann das Benutzerzertifikat CertU ermittelt. Das Benutzerzertifikat CertU kann z. B. aus einer der Zertifizierungscomputereinheit CA eigenen Datenbank ermittelt werden, die alle Zertifikate der Computereinheiten enthält, für die die Zertifizierungscomputereinheit CA Zertifikate erstellt.

Um die Gültigkeit des Netzzertifikats CertN und des Benutzerzertifikats CertU zu überprüfen, wird eine Identitätsangabe id_N und der in der vierten Nachricht mitgesendete öffentliche Netzschlüssel g^s, die Identitätsgröße IMUI der ersten Computereinheit U sowie das ermittelte Benutzerzertifikat CertU mit einer Revokationsliste verglichen, in der ungültige Zertifikate, Schlüssel oder Identitätsgrößen aufgeführt sind.

Anschließend wird aus mindestens einer Verkettung des ersten Werts g^t, des öffentlichen Netzschlüssels g^s und der Identitätsangabe id_N der zweiten Computereinheit N ein dritter Term gebildet.

Der dritte Term wird mit Hilfe einer vierten Hash-Funktion h4 "gehasht" und das Ergebnis der Hash-Funktion h4 wird unter Verwendung einer dritten Signaturfunktion Sig_{CA} signiert. Ein

Netzzertifikat CertN wird nun in der Zertifizierungscomputereinheit CA gebildet, wobei das Netzzertifikat CertN mindestens den dritten Term und den signierten Hash-Wert des dritten Terms aufweist.

Weiterhin wird beispielsweise in der Zertifizierungscomputereinheit CA ein Zeitstempel TS kreiert.

In der Zertifizierungscomputereinheit CA wird außerdem ein fünfter Term gebildet, der mindestens eine Verkettung des Zeitstempels TS, der Identitätsangabe id_N der zweiten Computereinheit N und des Benutzerzertifikats CertU aufweist.

Ein zweiter signierter Term wird gebildet durch Anwendung der dritten Signaturfunktion Sig_{CA} auf einen zweiten Signatureingangsterm und den geheimen Zertifizierungsschlüssel u. Der zweite Signatureingangsterm weist mindestens ein Ergebnis der vierten Hash-Funktion h4 auf, die auf mindestens den fünften Term angewendet wird.

Anschließend wird ein sechster Term gebildet, der mindestens den fünften Term und den signierten Hash-Wert des fünften Terms aufweist.

Eine in der Zertifizierungscomputereinheit CA gebildete fünfte Nachricht M5 weist mindestens eine Verkettung aus dem Netzzertifikat CertN und dem sechsten Term auf.

Die fünfte Nachricht M5 wird in der Zertifizierungscomputereinheit CA codiert und an die zweite Computereinheit N übertragen. Nachdem die fünfte Nachricht in der zweiten Computereinheit N decodiert ist, wird das Netzzertifikat CertN und der zweite signierte Term verifiziert.

In der zweiten Computereinheit N wird nun ein vierter Term gebildet, der mindestens eine Verkettung des öffentlichen

Netzschlüssels g^s und des signierten Hash-Werts des dritten Terms aufweist.

In der zweiten Computereinheit N wird mit Hilfe einer ersten Hash-Funktion h1 ein Sitzungsschlüssel K gebildet. Als eine erste Eingangsgröße der ersten Hash-Funktion h1 wird eine Konkatenation eines ersten Terms mit der zweiten Zufallszahl r verwendet. Der erste Term wird gebildet, indem der erste Wert g^t potenziert wird mit einem geheimen Netzschlüssel s. Unter einer Hash-Funktion ist in diesem Zusammenhang eine Funktion zu verstehen, bei der es nicht möglich ist, zu einem gegebenen Funktionswert einen passenden Eingangswert zu berechnen. Ferner wird einer beliebig langen Eingangszeichenfolge eine Ausgangszeichenfolge fester Länge zugeordnet. Des weiteren wird für die Hash-Funktion in diesem Zusammenhang Kollisionsfreiheit gefordert, d. h. es darf nicht möglich sein, zwei verschiedene Eingangszeichenfolgen zu finden, die dieselbe Ausgangszeichenfolge ergeben. Die zweite Zufallszahl r findet Verwendung, wie in den Figuren 2a, b beschrieben, wenn das zusätzliche Sicherheitsziel der Zusicherung der Frische (Aktualität) des Sitzungsschlüssels K für die zweiten Computereinheit N realisiert werden soll. Ist dieses Sicherheitsziel nicht benötigt, wird die zweite Zufallszahl r nicht in dem erfindungsgemäßen Verfahren verwendet.

Nun wird in der zweiten Computereinheit N eine Antwort A gebildet. Zur Bildung der Antwort A sind verschiedene Varianten vorgesehen. So ist es z. B. möglich, daß mit dem Sitzungsschlüssel K unter Verwendung einer Verschlüsselungsfunktion Enc eine Konstante const verschlüsselt wird. Die Konstante const ist sowohl der ersten Computereinheit U als auch der zweiten Computereinheit N bekannt. Auch die Verschlüsselungsfunktion Enc ist sowohl der zweiten Computereinheit N als auch der ersten Computereinheit U als die in dem erfindungsgemäßen Verfahren zu verwendende Verschlüsselungsfunktion bekannt.

Eine weitere Möglichkeit, die Antwort A zu bilden liegt z. B. darin, daß der Sitzungsschlüssel K als Eingangsgröße für eine dritte Hash-Funktion h3 verwendet wird und der "gehashte" Wert des Sitzungsschlüssels K als Antwort A verwendet wird. Weitere Möglichkeiten, die Antwort A zu bilden, die zur Überprüfung des Sitzungsschlüssels K in der ersten Computereinheit U verwendet wird, sind dem Fachmann geläufig und können als Varianten zu den beschriebenen Vorgehensweisen verwendet werden.

Eine Aneinanderreihung der zweiten Zufallszahl r, des vierten Terms der Antwort A, sowie ein optionales erstes Datenfeld dat1 bilden eine zweite Nachricht M2. Die zweite Zufallszahl r und das optionale erste Datenfeld dat1 sind nur in der zweiten Nachricht M3 enthalten, wenn diese in dem erfindungsgemäßen Verfahren vorgesehen werden.

Die zweite Nachricht M2 wird in der zweiten Computereinheit N codiert und zu der ersten Computereinheit U übertragen.

In der ersten Computereinheit U wird die zweite Nachricht M2 decodiert, so daß die ersten Computereinheit U eventuell die zweite Zufallszahl r, die Antwort A sowie eventuell das optionale erste Datenfeld dat1 zur Verfügung hat. Die Länge des optionalen ersten Datenfeldes dat1 kann beliebig groß sein, d. h. es ist auch möglich, daß das optionale erste Datenfeld dat1 nicht vorhanden ist.

In der ersten Computereinheit U wird nun ebenfalls der Sitzungsschlüssel K gebildet, mit Hilfe der ersten Hash-Funktion h1, die sowohl der zweiten Computereinheit N als auch der ersten Computereinheit U bekannt ist. Eine zweite Eingangsgröße der ersten Hash-Funktion h1 zur Bildung des Sitzungsschlüssels K in der ersten Computereinheit U weist mindestens einen zweiten Term auf. Der zweite Term wird gebildet aus einer Exponentation eines öffentlichen Netzschlüssels g^s mit der ersten Zufallszahl t. Wenn die zweite Zufallszahl r in dem er-

findungsgemäßen Verfahren vorgesehen wird, so weist die zweite Eingangsgröße der ersten Hash-Funktion h1 zur Bildung des Sitzungsschlüssels K in der ersten Computereinheit U zusätzlich die zweite Zufallszahl r auf.

Durch die Verwendung der ersten Zufallszahl t und der zweiten Zufallszahl r bei der Generierung des Sitzungsschlüssels K wird die Aktualität des Sitzungsschlüssels K gewährleistet, da jeweils die erste Zufallszahl t als auch die zweite Zufallszahl r nur für jeweils einen Sitzungsschlüssel K verwendet werden.

Somit wird eine Wiedereinspielung eines älteren Schlüssels als Sitzungsschlüssel K verhindert. Wenn aber für jeden neuen Sitzungsschlüssel K andere Zufallszahlen verwendet werden, so ist die Wahrscheinlichkeit, daß der verwendete Sitzungsschlüssel K von einem unbefugten Dritten schon herausgefunden wurde, wesentlich geringer. Damit ist die Gefahr, daß der Teil einer Nachricht, der mit dem Sitzungsschlüssel K verschlüsselt ist, von einem unbefugten Dritten entschlüsselt werden kann, erheblich reduziert.

Nachdem in der ersten Computereinheit U der Sitzungsschlüssel K gebildet wurde, wird anhand der empfangenen Antwort A überprüft, ob der in der ersten Computereinheit U gebildete Sitzungsschlüssel K mit dem Sitzungsschlüssel K, der in der zweiten Computereinheit N gebildet wurde, übereinstimmt.

Abhängig von den im vorigen beschriebenen Varianten zur Bildung der Antwort A sind verschiedene Möglichkeiten vorgesehen, den Sitzungsschlüssel K anhand der Antwort A zu überprüfen.

Eine Möglichkeit besteht z. B. darin, daß, wenn die Antwort A in der zweiten Computereinheit N durch Verschlüsselung der Konstante const mit dem Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc gebildet wurde, die Antwort

A entschlüsselt wird, und somit die ersten Computereinheit U eine entschlüsselte Konstante const' erhält, die mit der bekannten Konstante const verglichen wird.

Die Überprüfung des Sitzungsschlüssels K anhand der Antwort A kann auch durchgeführt werden, indem die der ersten Computereinheit U bekannte Konstante const mit dem in der ersten Computereinheit U gebildeten Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc verschlüsselt wird und das Ergebnis mit der Antwort A auf Übereinstimmung geprüft wird. Diese Vorgehensweise wird z. B. auch verwendet, wenn die Antwort A in der zweiten Computereinheit N gebildet wird, indem auf den Sitzungsschlüssel K die dritte Hash-Funktion h3 angewendet wird. In diesem Fall wird in der ersten Computereinheit U der in der ersten Computereinheit U gebildete Sitzungsschlüssel K als Eingangsgröße der dritten Hash-Funktion h3 verwendet. Der "gehashte" Wert des in der ersten Computereinheit U gebildeten Sitzungsschlüssel K wird dann mit der Antwort A auf Übereinstimmung geprüft. Damit wird das Ziel der Schlüsselbestätigung des Sitzungsschlüssels K erreicht.

Dadurch, daß bei der Berechnung des Sitzungsschlüssels K in der zweiten Computereinheit N der geheime Netzschlüssel s und bei der Berechnung des Sitzungsschlüssels K in der ersten Computereinheit U der öffentliche Netzschlüssel g^s verwendet werden, wird die zweiten Computereinheit N durch die ersten Computereinheit U authentifiziert. Dies wird erreicht, vorausgesetzt daß für die ersten Computereinheit U bekannt ist, daß der öffentliche Netzschlüssel g^s tatsächlich zur zweiten Computereinheit N gehört.

Im Anschluß an die Bestätigung des Sitzungsschlüssels K durch Überprüfung der Antwort A wird ein Signaturterm berechnet. Hierzu wird mit Hilfe einer zweiten Hash-Funktion h2 eine vierte Eingangsgröße gebildet. Die zweite Hash-Funktion h2 kann, muß aber nicht dieselbe Hash-Funktion sein wie die er-

ste Hash-Funktion h1. Als eine dritte Eingangsgröße für die zweite Hash-Funktion h2 wird ein Term verwendet, der mindestens den Sitzungsschlüssel K enthält. Weiterhin kann die dritte Eingangsgröße das optionale erste Datenfeld dat1 oder auch ein optionales zweites Datenfeld dat2 enthalten, wenn deren Verwendung in dem erfindungsgemäßen Verfahren vorgesehen wird.

Es kann später nicht abgestritten werden, daß die Daten, die im ersten optionale Datenfeld dat1 und im zweiten optionalen Datenfeld dat2 enthalten sind, von der ersten Computereinheit U gesendet werden.

Die in dem ersten optionalen Datenfeld dat1 und in dem zweiten optionalen Datenfeld dat2 enthaltenen Daten können z. B. Telefonnummern, die aktuelle Zeit oder ähnliche hierfür geeignete Parameter sein. Diese Information kann als Werkzeug für eine unanfechtbare Gebührenabrechnung verwendet werden.

Unter Verwendung einer ersten Signaturfunktion Sig_U wird der Signaturterm aus mindestens der vierten Eingangsgröße gebildet. Um einen höheren Sicherheitsgrad zu erzielen, kann der Signaturterm verschlüsselt werden. Der Signaturterm wird in diesem Fall mit dem Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc verschlüsselt und bildet den ersten verschlüsselten Term VT1.

Bei Verwendung eines optionalen zweiten Datenfeldes dat2 wird in der ersten Computereinheit U ein dritter verschlüsselter Term VT3 berechnet, indem das optionale zweite Datenfeld dat2 mit dem Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc verschlüsselt wird. Das optionale zweite Datenfeld dat2 kann auch unverschlüsselt, also im Klartext übertragen werden.

In der ersten Computereinheit U wird eine dritte Nachricht M3 gebildet und codiert, die mindestens aus dem ersten ver-

schlüsselten Term VT1, und, wenn das optionale zweite Datenfeld dat2 verwendet wird, dem dritten verschlüsselten Term VT3 oder dem optionalen zweiten Datenfeld dat2 im Klartext besteht. Die dritte Nachricht M3 wird von der ersten Computereinheit U zu der zweiten Computereinheit N übertragen.

Zusätzlich wird die Authentifikation der ersten Computereinheit U gegenüber der zweiten Computereinheit N durch den Signaturterm in der dritten Nachricht M3 gewährleistet, durch deren Verwendung auch garantiert wird, daß die dritte Nachricht M3 tatsächlich aktuell von der ersten Computereinheit U gesendet wurde.

In der zweiten Computereinheit N wird die dritte Nachricht M3 decodiert und anschließend wird der erste verschlüsselte Term VT1 sowie eventuell der dritte verschlüsselte Term VT3 entschlüsselt. Anhand des Benuterzertifikats CertU, das der zweiten Computereinheit N zur Verfügung steht, wird der Signaturterm verifiziert.

Wenn die Verwendung des optionalen zweiten Datenfelds dat2 vorgesehen wird, weist die dritte Nachricht M3 zusätzlich mindestens den dritten verschlüsselten Term VT3 auf oder das optionale zweite Datenfeld dat2 in Klartext, wenn das optionale zweite Datenfeld dat2 in Klartext übertragen werden soll.

Wenn die dritte Nachricht M3 den ersten verschlüsselten Term VT1, den zweiten verschlüsselten Term VT2 oder den dritten verschlüsselten Term VT3 aufweist, werden diese in der zweiten Computereinheit N entschlüsselt. Dies geschieht für den eventuell vorhandenen ersten verschlüsselten Term VT1 vor der Verifikation des Signaturterms.

Wenn für das erfindungsgemäße Verfahren temporäre Benutzeridentitäten vorgesehen werden, so wird das im vorigen beschriebene Verfahren um einige Verfahrensschritte erweitert.

In der zweiten Computereinheit N wird für die erste Computereinheit U eine neue temporäre Identitätsgröße TMUIN gebildet, die der ersten Computereinheit U im weiteren zugewiesen wird. Dies kann z. B. durch Generierung einer Zufallszahl oder durch Tabellen, in denen mögliche Identitätsgrößen abgespeichert sind, durchgeführt werden. Aus der neuen temporären Identitätsgröße TMUIN der ersten Computereinheit U wird in der zweiten Computereinheit N ein vierter verschlüsselter Term VT4 gebildet, indem die neue temporäre Identitätsgröße TMUIN der ersten Computereinheit U mit dem Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc verschlüsselt wird.

In diesem Fall weist die zweite Nachricht M2 zusätzlich mindestens den vierten verschlüsselten Term VT4 auf. Der vierte verschlüsselte Term VT4 wird dann in der ersten Computereinheit U entschlüsselt. Nun ist die neue temporäre Identitätsgröße TMUIN der ersten Computereinheit U in der ersten Computereinheit U verfügbar.

Damit der zweiten Computereinheit N auch gewährleistet wird, daß die erste Computereinheit U die neue temporäre Identitätsgröße TMUIN korrekt empfangen hat, weist die dritte Eingangsgröße für die erste Hash-Funktion h1 oder für die zweite Hash-Funktion h2 zusätzlich mindestens die neue temporäre Identitätsgröße TMUIN der ersten Computereinheit U auf.

Patentansprüche

1. Verfahren zum rechnergestützten Austausch kryptographischer Schlüssel zwischen einer ersten Computereinheit (U) und einer zweiten Computereinheit (N),

- bei dem aus einer ersten Zufallszahl (t) mit Hilfe eines erzeugenden Elements (g) einer endlichen Gruppe in der ersten Computereinheit (U) ein erster Wert (g^t) gebildet wird,
- bei eine erste Nachricht (M1) von der ersten Computereinheit (U) an die zweite Computereinheit (N) übertragen wird, wobei die ersten Nachricht (M1) mindestens den ersten Wert (g^t) aufweist,
- bei dem in der zweite Computereinheit (N) ein Sitzungsschlüssel (K) mit Hilfe einer ersten Hash-Funktion (h1) gebildet wird, wobei eine erste Eingangsgröße der ersten Hash-Funktion (h1) mindestens einen ersten Term aufweist, der gebildet wird durch eine Exponentiation des ersten Werts (g^t) mit einem geheimen Netzschlüssel (s),
- bei dem in der ersten Computereinheit (U) der Sitzungsschlüssel (K) gebildet wird mit Hilfe der ersten Hash-Funktion (h1), wobei eine zweite Eingangsgröße der ersten Hash-Funktion (h1) mindestens einen zweiten Term aufweist, der gebildet wird durch eine Exponentiation eines öffentlichen Netzschlüssels (g^s) mit der ersten Zufallszahl (t),
- bei dem in der ersten Computereinheit (U) mit Hilfe einer zweiten Hash-Funktion (h2) oder der ersten Hash-Funktion (h1) eine vierte Eingangsgröße gebildet wird, wobei eine dritte Eingangsgröße für die erste Hash-Funktion (h1) oder für die zweite Hash-Funktion (h2) zur Bildung der vierten Eingangsgröße mindestens den Sitzungsschlüssel (K) aufweist,
- bei dem in der ersten Computereinheit (U) ein Signaturterm aus mindestens der vierten Eingangsgröße gebildet wird unter Anwendung einer ersten Signaturfunktion (Sig_U),
- bei dem eine dritte Nachricht (M3) von der ersten Computereinheit (U) an die zweite Computereinheit (N) übertragen

wird, wobei die dritte Nachricht (M3) mindestens den Signaturterm der ersten Computereinheit (U) aufweist, und

- bei dem in der zweiten Computereinheit (N) der Signaturterm verifiziert wird.

2. Verfahren nach Anspruch 1,

- bei dem die erste Nachricht (M1) zusätzlich eine Identitätsangabe (id_{CA}) einer Zertifizierungscomputereinheit (CA), die ein Netzzertifikat (CertN) liefert, das von der ersten Computereinheit (U) verifiziert werden kann, aufweist,
- bei dem eine zweite Nachricht (M2) von der zweiten Computereinheit (N) an die erste Computereinheit (U) übertragen wird, wobei die zweite Nachricht (M2) mindestens das Netzzertifikat (CertN) aufweist, und
- bei dem in der ersten Computereinheit (U) das Netzzertifikat (CertN) verifiziert wird.

3. Verfahren nach Anspruch 2,

- bei dem eine dritte Nachricht (M3) von der ersten Computereinheit (U) an die zweite Computereinheit (N) übertragen wird, wobei die dritte Nachricht (M3) zusätzlich ein Benutzerzertifikat (CertU) aufweist,
- bei dem in der zweiten Computereinheit (N) das Benutzerzertifikat (CertU) verifiziert wird.

4. Verfahren nach Anspruch 1,

- bei dem die erste Nachricht (M1) zusätzlich eine Identitätsgröße (IMUI) der ersten Computereinheit (U) und eine Identitätsangabe (id_{CA}) einer Zertifizierungscomputereinheit (CA), die der ersten Computereinheit (U) ein Netzzertifikat (CertN) liefert, das von der ersten Computereinheit (U) verifiziert werden kann, aufweist,
- bei dem eine vierte Nachricht (M4) von der zweiten Computereinheit (N) an die Zertifizierungscomputereinheit (CA) übertragen wird, wobei die vierte Nachricht (M4) mindestens den öffentlichen Netzschlüssel (g^s), den ersten Wert (g^t),

die Identitätsgröße (IMUI) der ersten Computereinheit (U) als Eingangsgröße aufweist und wobei eine Ausgangsgröße einer dritten Hash-Funktion (h3) unter Verwendung einer zweiten Signaturfunktion (Sig_N) signiert wird,

- bei dem in der Zertifizierungscomputereinheit (CA) der erste signierte Term verifiziert wird,
- bei dem in der Zertifizierungscomputereinheit (CA) ein dritter Term gebildet wird, der mindestens den ersten Wert (g^t), den öffentlichen Netzschlüssel (g^s) und eine Identitätsangabe (id_N) der zweiten Computereinheit (N) aufweist,
- bei dem in der Zertifizierungscomputereinheit (CA) unter Verwendung einer vierten Hash-Funktion (h4) ein Hash-Wert über den dritten Term gebildet wird,
- bei dem in der Zertifizierungscomputereinheit (CA) der Hash-Wert über den dritten Term unter Verwendung einer dritten Signaturfunktion (Sig_{CA}) mit einem geheimen Zertifizierungsschlüssel (U) signiert wird,
- bei dem in der Zertifizierungscomputereinheit (CA) ein Netzzertifikat (CertN) gebildet wird, das mindestens den dritten Term und den signierten Hash-Wert des dritten Terms aufweist,
- bei dem in der Zertifizierungscomputereinheit (CA) auf einen fünften Term der mindestens die Identitätsangabe (id_N) der zweiten Computereinheit (N) und ein Benutzerzertifikat (CertU) aufweist, eine vierte Hash-Funktion (h4) angewendet wird,
- bei dem der Hash-Wert des fünften Terms durch Verwendung der dritten Signaturfunktion (Sig_{CA}) mit dem geheimen Zertifizierungsschlüssel (cs) signiert und das Ergebnis den zweiten signierten Term darstellt,
- bei dem eine fünfte Nachricht (M5), die mindestens das Netzzertifikat (CertN), den fünften Term und den zweiten signierten Term aufweist, von der Zertifizierungscomputereinheit (CA) zu der zweiten Computereinheit (N) übertragen wird,

- bei dem in der zweiten Computereinheit (N) das Netzzertifikat (CertN) und der zweite signierte Term verifiziert werden,
- bei dem in der zweiten Computereinheit (N) ein vierter Term, der mindestens den öffentlichen Netzschlüssel (g^S) und den signierten Hash-Wert des dritten Terms aufweist, gebildet wird,
- bei dem eine zweite Nachricht (M2) von der zweiten Computereinheit (N) an die erste Computereinheit (U) übertragen wird, wobei die zweite Nachricht (M2) mindestens den vierten Term aufweist, und
- bei dem in der ersten Computereinheit (U) das Netzzertifikat (CertN) verifiziert wird.

5. Verfahren nach Anspruch 4,
bei dem der fünfte Term zusätzlich einen Zeitstempel (TS) aufweist.

6. Verfahren nach Anspruch 4 oder 5,
- bei dem in der ersten Computereinheit (U) vor Bildung der ersten Nachricht (M1) ein Zwischenschlüssel (L) gebildet wird, indem ein öffentlicher Zertifizierungsschlüssel (g^U) mit der ersten Zufallszahl (t) potenziert wird,
- bei dem in der ersten Computereinheit (U) vor Bildung der ersten Nachricht (M1) aus der Identitätsgröße (IMUI) der ersten Computereinheit (U) ein zweiter verschlüsselter Term (VT2) gebildet wird, indem die Identitätsgröße (IMUI) mit dem Zwischenschlüssel (L) unter Anwendung einer Verschlüsselungsfunktion (Enc) verschlüsselt wird,
- bei dem die erste Nachricht (M1) anstatt der Identitätsgröße (IMUI) der ersten Computereinheit(U) den zweiten verschlüsselten Term (VT2) aufweist,
- bei dem die vierte Nachricht (M4) anstatt der Identitätsgröße (IMUI) der ersten Computereinheit (U) den zweiten verschlüsselten Term (VT2) aufweist, und

- bei dem in der Zertifizierungscomputereinheit (CA), nachdem die vierte Nachricht (M4) empfangen wurde, der zweite verschlüsselte Term (VT2) entschlüsselt wird.

7. Verfahren nach einem der Ansprüche 4 bis 6, bei dem in der Zertifizierungscomputereinheit (CA) mindestens eine der Größen, die Identitätsangabe (id_N) der zweiten Computereinheit (N), die Identitätsgröße ($|MU|$) der ersten Computereinheit (U), der öffentliche Netzschlüssel (g^S) oder das Benutzerzertifikat (CertU) anhand einer Revokationsliste überprüft wird.

8. Verfahren nach einem der Ansprüche 1 bis 7,

- bei dem die erste Nachricht (M1) zusätzlich mindestens eine alte temporäre Identitätsgröße (TMUIO) der ersten Computereinheit (U) aufweist,
- bei dem in der zweiten Computereinheit (N), nach dem die ersten Nachricht (M1) empfangen wurde und bevor die zweite Nachricht (M2) gebildet wird, für die erste Computereinheit (U) eine neue temporäre Identitätsgröße (TMUIN) gebildet wird,
- bei dem aus der neuen temporären Identitätsgröße (TMUIN) der ersten Computereinheit (U) ein vierter verschlüsselter Term (VT4) gebildet wird, in dem die neue temporäre Identitätsgröße (TMUIN) der ersten Computereinheit (U) mit dem Sitzungschlüssel (K) unter Anwendung der Verschlüsselungsfunktion (Enc) verschlüsselt wird,
- bei dem die zweite Nachricht (M2) zusätzlich mindestens den vierten verschlüsselten Term (VT4) aufweist,
- bei dem in der ersten Computereinheit (U), nachdem die zweite Nachricht (M2) empfangen wurde und bevor die vierte Eingangsgröße gebildet wird, der vierte verschlüsselte Term (VT4) entschlüsselt wird,
- bei dem die dritte Eingangsgröße für die erste Hash-Funktion (h1) oder für die zweite Hash-Funktion (h2) zur Bildung der vierten Eingangsgröße zusätzlich mindestens die neue

temporäre Identitätsgröße (TMUIN) der ersten Computereinheit (U) aufweist, und

- bei dem die dritte Nachricht (M3) nicht die Identitätsgröße (IMUI) der ersten Computereinheit (U) aufweist.

9. Verfahren nach einem der Ansprüche 1 bis 8,

- bei dem in der zweiten Computereinheit (N) eine Information zu dem Sitzungsschlüssel (K) enthaltende Antwort (A) gebildet wird,
- bei dem eine zweite Nachricht (M2) von der zweite Computereinheit (N) an die erste Computereinheit (U) übertragen wird, wobei die zweite Nachricht (M2) mindestens die Antwort (A) aufweist, und
- bei dem in der ersten Computereinheit (U) der Sitzungsschlüssel (K) anhand der Antwort (A) überprüft wird.

10. Verfahren nach Anspruch 9,
bei dem die dritte Nachricht (M3) zusätzlich eine Identitätsgröße (IMUI) der ersten Computereinheit aufweist.

11. Verfahren nach einem der Ansprüche 1 bis 10,

- bei dem in der zweiten Computereinheit (N) die erste Eingangsgröße der ersten Hash-Funktion (h1) zusätzlich mindestens eine zweite Zufallszahl (r) aufweist,
- bei dem die zweite Nachricht (M2) zusätzlich die zweite Zufallszahl (r) aufweist, und
- bei dem in der ersten Computereinheit (U) die zweite Eingangsgröße der ersten Hash-Funktion (h1) zusätzlich mindestens die zweite Zufallszahl (r) aufweist.

12. Verfahren nach einem der Anschlüsse 1 bis 5,

- bei dem in der ersten Computereinheit (U) vor Bildung der dritten Nachricht (M3) aus der Identitätsgröße (IMUI) der ersten Computereinheit (U) ein zweiter verschlüsselter Term (VT2) gebildet wird, in dem die Identitätsgröße (IMUI) mit dem Sitzungsschlüssel (K) unter Anwendung der Verschlüsselungsfunktion (Enc) verschlüsselt wird,

- bei dem die dritte Nachricht (M3) zusätzlich den zweiten verschlüsselten Term (VT2) aufweist, und
- bei dem in der zweiten Computereinheit (N), nachdem die dritte Nachricht (M3) empfangen wurde, der zweite verschlüsselte Term (VT2) entschlüsselt wird.

13. Verfahren nach einem der Ansprüche 1 bis 12,
- bei dem die zweite Nachricht (M2) zusätzlich ein optionales erstes Datenfeld (dat1) aufweist und
- bei dem die dritte Eingangsgröße für die erste Hash-Funktion (h1) oder für die zweite Hash-Funktion (h2) zur Bildung der vierten Eingangsgröße zusätzlich mindestens das optionale erste Datenfeld (dat1) aufweist.

14. Verfahren nach einem der Ansprüche 1 bis 13,
- bei dem in der ersten Computereinheit (U) vor Bildung der dritten Nachricht (M3) ein dritter verschlüsselter Term (VT3) gebildet wird, indem ein optionales zweites Datenfeld (dat2) mit dem Sitzungsschlüssel (K) unter Anwendung der Verschlüsselungsfunktion (Enc) verschlüsselt wird,
- bei dem die dritte Nachricht (M3) zusätzlich mindestens den dritten verschlüsselten Term (VT3) aufweist, und
- bei dem in der zweiten Computereinheit (N), nachdem die dritte Nachricht (M3) empfangen wurde, der dritte verschlüsselte Term (VT3) entschlüsselt wird.

15. Verfahren nach einem der Ansprüche 1 bis 14,
- bei dem in der ersten Computereinheit (U) vor Bildung der dritten Nachricht (M3) ein erster verschlüsselter Term (VT1) gebildet wird, indem der Signaturterm mit dem Sitzungsschlüssel (K) unter Anwendung der Verschlüsselungsfunktion (Enc) verschlüsselt wird,
- bei dem die dritte Nachricht (M3) zusätzlich den ersten verschlüsselten Term (VT1) aufweist, und
- bei dem in der zweiten Computereinheit (N), nachdem die dritte Nachricht (M3) empfangen wurde und bevor der Signa-

turterm verifiziert wird, der erste verschlüsselte Term (VT1) entschlüsselt wird.

16. Verfahren nach einem der Ansprüche 1 bis 15, bei dem in der zweiten Computereinheit (N) eine Antwort (A) gebildet wird, indem eine Konstante (const), die in der zweiten Computereinheit (N) und in der ersten Computereinheit (U) bekannt sind, mit dem Sitzungsschlüssel (K) unter Anwendung der Verschlüsselungsfunktion (Enc) verschlüsselt wird.

17. Verfahren nach einem der Ansprüche 1 bis 16,
- bei dem in der zweiten Computereinheit (N) eine Antwort (A) gebildet wird, indem auf den Sitzungsschlüssel (K) eine dritte Hash-Funktion (h3) angewendet wird, und
- bei dem in der ersten Computereinheit (U) die Antwort (A) überprüft wird, indem auf den Sitzungsschlüssel (K) die dritte Hash-Funktion (h3) angewendet wird, und das Ergebnis mit der Antwort (A) verglichen wird.

18. Verfahren nach einem der Ansprüche 9 bis 15 oder 17, bei dem in der ersten Computereinheit (U) die Antwort (A) überprüft wird, indem eine Konstante (const) mit dem Sitzungsschlüssel (K) unter Anwendung der Verschlüsselungsfunktion (Enc) verschlüsselt wird und das Ergebnis mit der Antwort (A) verglichen wird.

19. Verfahren nach einem der Ansprüche 9 bis 15 oder 17, bei dem in der ersten Computereinheit (U) die Antwort (A) überprüft wird, indem die Antwort (A) mit dem Sitzungsschlüssel (K) unter Anwendung der Verschlüsselungsfunktion (Enc) entschlüsselt wird und eine entschlüsselte Konstante (const') mit einer Konstante (const) verglichen wird.

20. Verfahren nach einem der Ansprüche 1 bis 19, bei dem die dritte Nachricht (M3) zusätzlich mindestens ein optionales zweites Datenfeld (dat2) aufweist.

21. Verfahren nach einem der Ansprüche 1 bis 20, bei dem die erste Computereinheit (U) durch ein mobiles Kommunikationsendgerät und/oder die zweite Computereinheit (N) durch eine Authentifizierungseinheit in einem Mobil-Kommunikationsnetz gebildet werden.

FIG 1

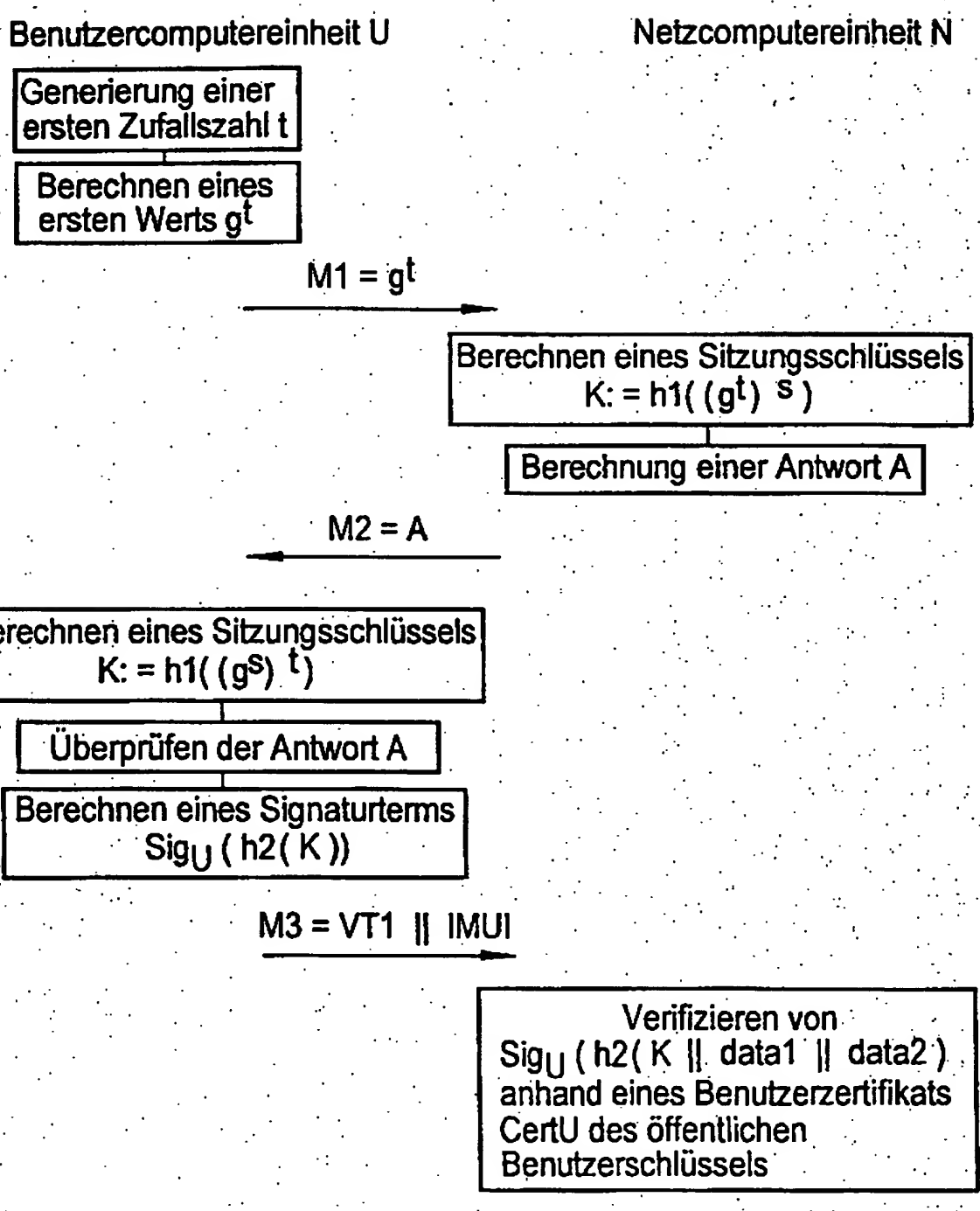

Benutzercomputereinheit U
Netzcomputereinheit N
Generierung einer ersten Zufallszahl t
Berechnen eines ersten Werts g^t
M1 = g^t
Berechnen eines Sitzungsschlüssels K: = h1((g^t) ^{s})
Berechnung einer Antwort A
M2 = A
Berechnen eines Sitzungsschlüssels K: = h1((g^s) ^{t})
Überprüfen der Antwort A
Berechnen eines Signaturterms Sig_U (h2(K))
M3 = VT1 || IMUI
Verifizieren von Sig_U (h2(K || data1 || data2) anhand eines Benutzerzertifikats CertU des öffentlichen Benutzerschlüssels

FIG 2

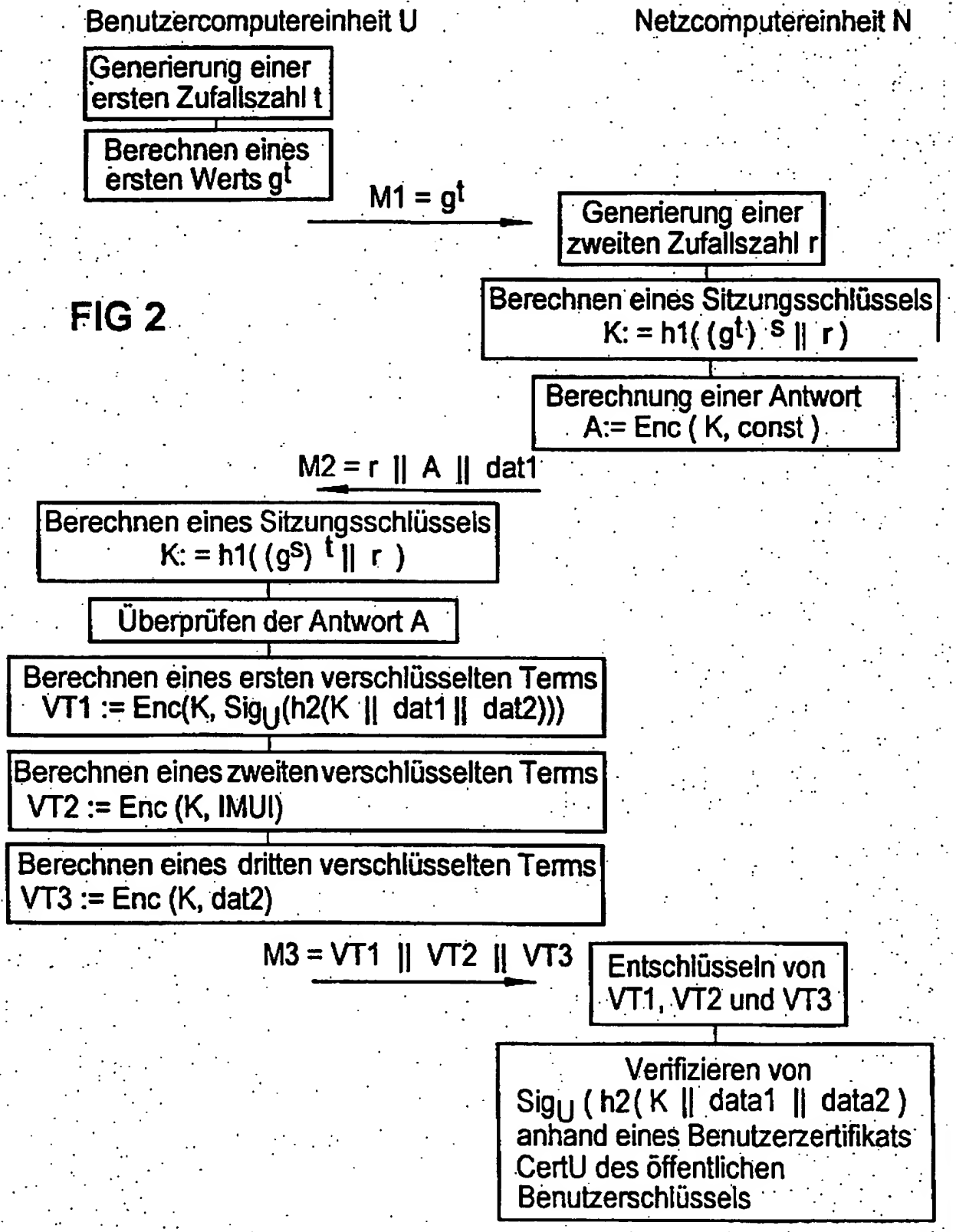
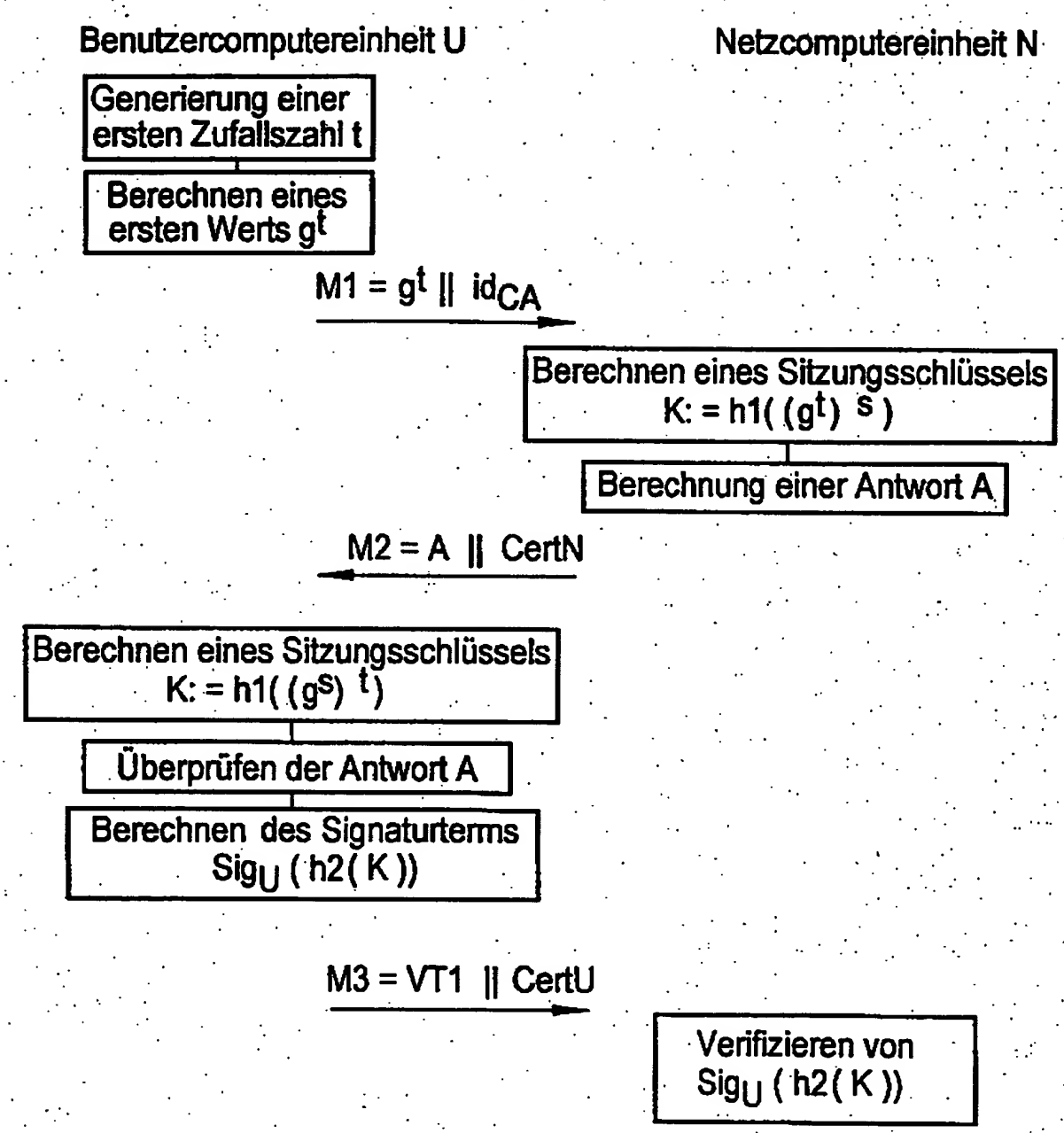

Benutzercomputereinheit U
Netzcomputereinheit N
Generierung einer ersten Zufallszahl t
Berechnen eines ersten Werts g^t
$M1 = g^t$
Generierung einer zweiten Zufallszahl r
Berechnen eines Sitzungsschlüssels $K: = h1((g^t)^s \| r)$
Berechnung einer Antwort A:= Enc (K, const)
M2 = r || A || dat1
Berechnen eines Sitzungsschlüssels $K: = h1((g^s)^t \| r)$
Überprüfen der Antwort A
Berechnen eines ersten verschlüsselten Terms $VT1 := Enc(K, Sig_U(h2(K \| dat1 \| dat2)))$
Berechnen eines zweiten verschlüsselten Terms VT2 := Enc (K, IMUI)
Berechnen eines dritten verschlüsselten Terms VT3 := Enc (K, dat2)
M3 = VT1 || VT2 || VT3
Entschlüsseln von VT1, VT2 und VT3
Verifizieren von $Sig_U (h2(K \| data1 \| data2)$ anhand eines Benutzerzertifikats CertU des öffentlichen Benutzerschlüssels

FIG 3


Benutzercomputereinheit U
Netzcomputereinheit N
Generierung einer ersten Zufallszahl t
Berechnen eines ersten Werts g^t
$M1 = g^t \| id_{CA}$
Berechnen eines Sitzungsschlüssels $K: = h1((g^t)^s)$
Berechnung einer Antwort A
$M2 = A \| CertN$
Berechnen eines Sitzungsschlüssels $K: = h1((g^s)^t)$
Überprüfen der Antwort A
Berechnen des Signaturterms $Sig_U(h2(K))$
$M3 = VT1 \| CertU$
Verifizieren von $Sig_U(h2(K))$

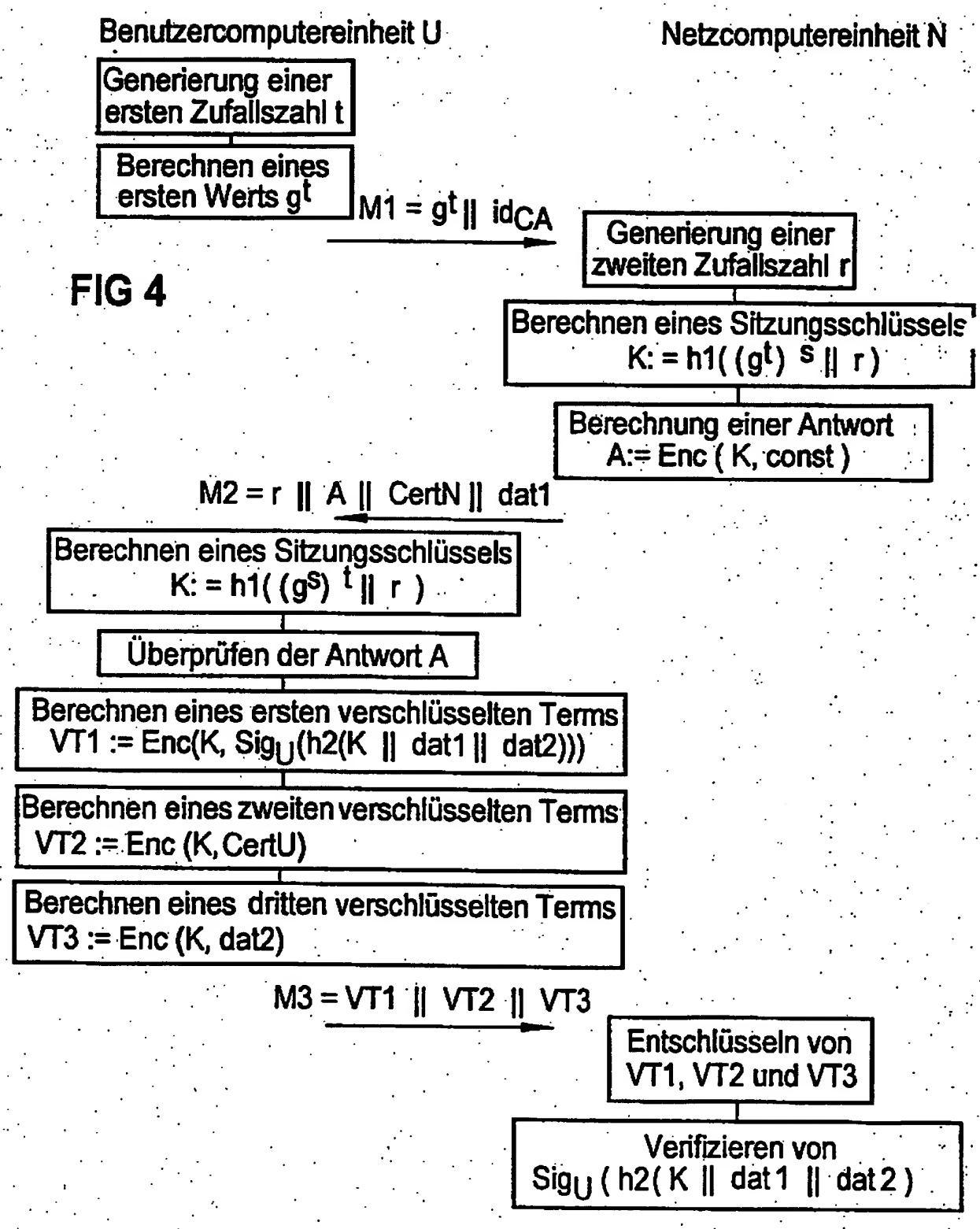

Benutzercomputereinheit U
Netzcomputereinheit N
Generierung einer ersten Zufallszahl t
Berechnen eines ersten Werts g^t
$M1 = g^t \| id_{CA}$
Generierung einer zweiten Zufallszahl r
Berechnen eines Sitzungsschlüssels $K := h1((g^t)^s \| r)$
Berechnung einer Antwort A:= Enc (K, const)
$M2 = r \| A \| CertN \| dat1$
Berechnen eines Sitzungsschlüssels $K := h1((g^s)^t \| r)$
Überprüfen der Antwort A
Berechnen eines ersten verschlüsselten Terms $VT1 := Enc(K, Sig_U(h2(K \| dat1 \| dat2)))$
Berechnen eines zweiten verschlüsselten Terms VT2 := Enc (K, CertU)
Berechnen eines dritten verschlüsselten Terms VT3 := Enc (K, dat2)
$M3 = VT1 \| VT2 \| VT3$
Entschlüsseln von VT1, VT2 und VT3
Verifizieren von $Sig_U (h2(K \| dat1 \| dat2)$

FIG 4

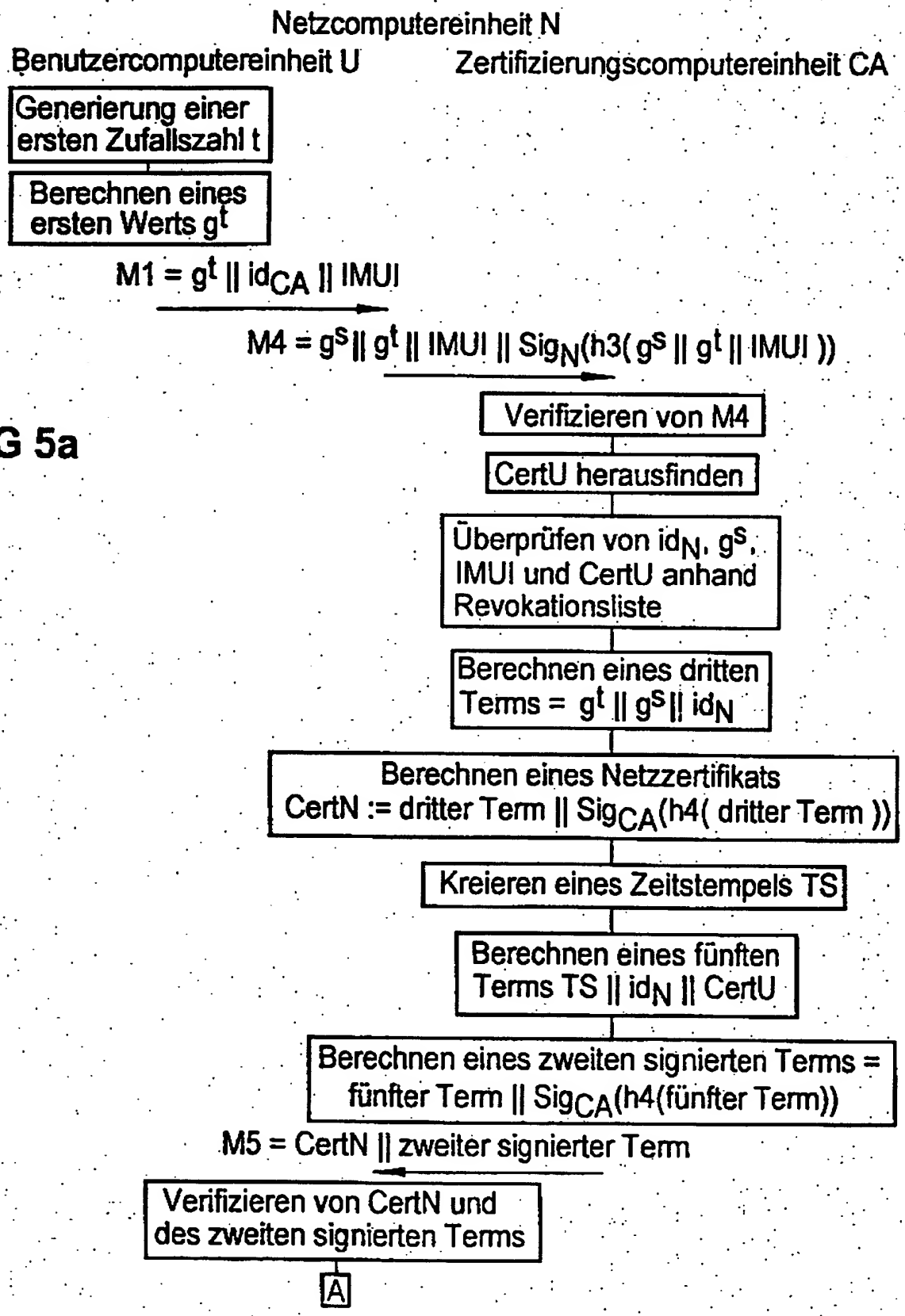
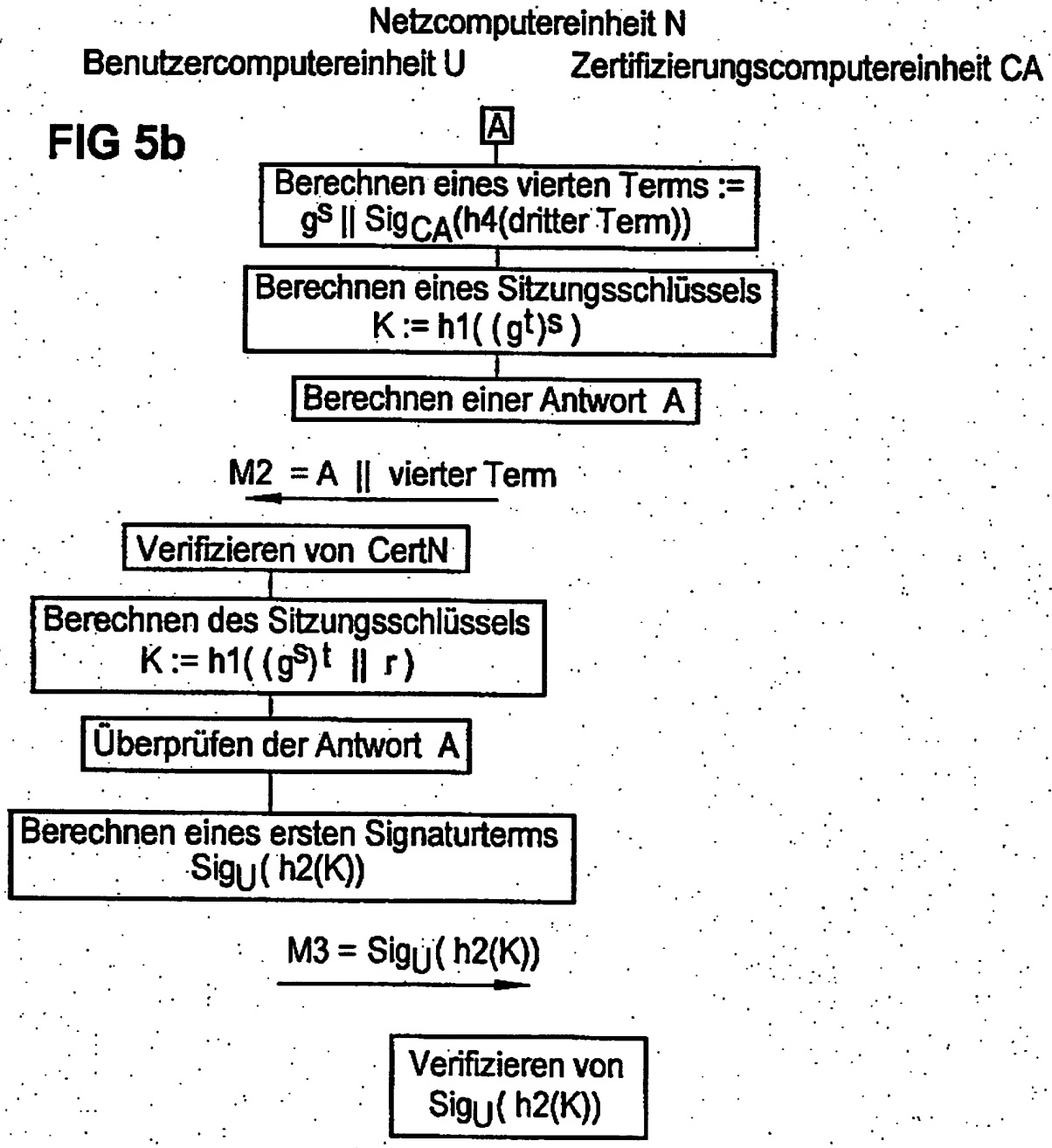

Netzcomputereinheit N
Benutzercomputereinheit U
Zertifizierungscomputereinheit CA
Generierung einer ersten Zufallszahl t
Berechnen eines ersten Werts g^t
$M1 = g^t \| id_{CA} \| IMUI$
$M4 = g^s \| g^t \| IMUI \| Sig_N(h3(g^s \| g^t \| IMUI))$
Verifizieren von M4
CertU herausfinden
Überprüfen von id_N, g^s, IMUI und CertU anhand Revokationsliste
Berechnen eines dritten Terms = $g^t \| g^s \| id_N$
Berechnen eines Netzzertifikats CertN := dritter Term $\| Sig_{CA}$(h4(dritter Term))
Kreieren eines Zeitstempels TS
Berechnen eines fünften Terms TS $\| id_N \|$ CertU
Berechnen eines zweiten signierten Terms = fünfter Term $\| Sig_{CA}$(h4(fünfter Term))
M5 = CertN || zweiter signierter Term
Verifizieren von CertN und des zweiten signierten Terms
A

FIG 5a

FIG 5b


Netzcomputereinheit N
Benutzercomputereinheit U
Zertifizierungscomputereinheit CA
A
Berechnen eines vierten Terms := g^s || Sig_{CA}(h4(dritter Term))
Berechnen eines Sitzungsschlüssels K := h1($(g^t)^s$)
Berechnen einer Antwort A
M2 = A || vierter Term
Verifizieren von CertN
Berechnen des Sitzungsschlüssels K := h1($(g^s)^t$ || r)
Überprüfen der Antwort A
Berechnen eines ersten Signaturterms Sig_U(h2(K))
M3 = Sig_U(h2(K))
Verifizieren von Sig_U(h2(K))

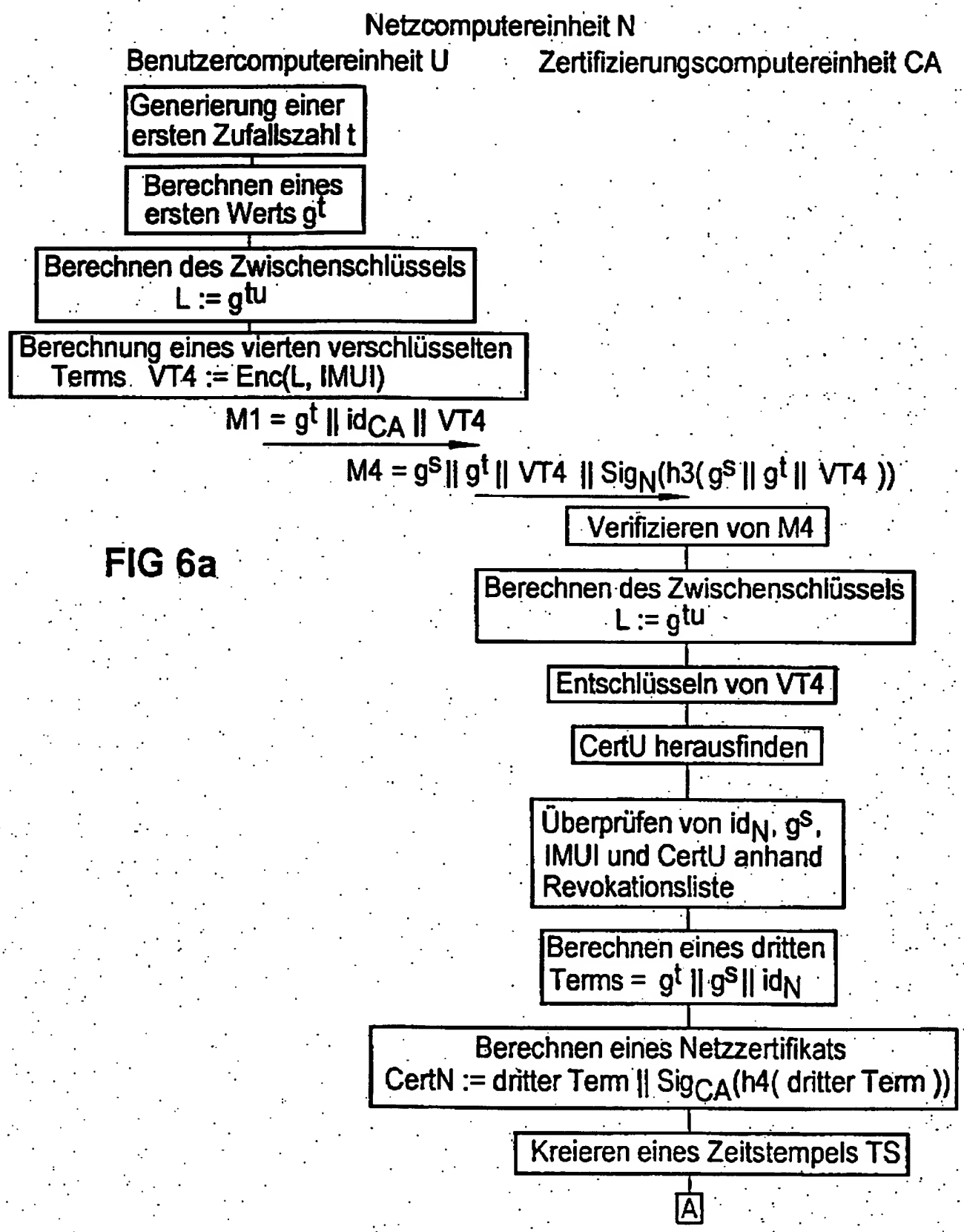
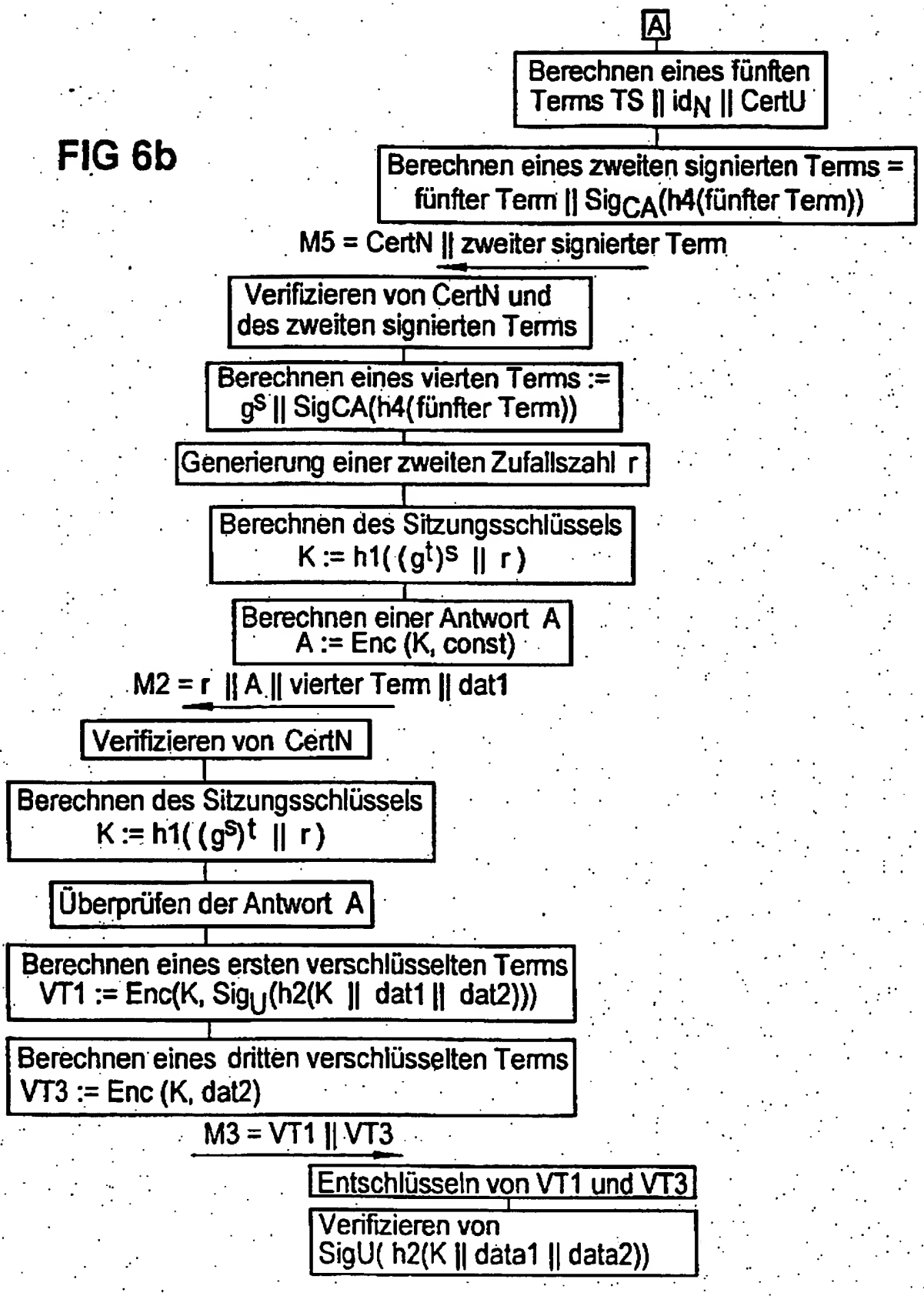

Netzcomputereinheit N
Benutzercomputereinheit U
Zertifizierungscomputereinheit CA
Generierung einer ersten Zufallszahl t
Berechnen eines ersten Werts g^t
Berechnen des Zwischenschlüssels $L := g^{tu}$
Berechnung eines vierten verschlüsselten Terms VT4 := Enc(L, IMUI)
$M1 = g^t \| id_{CA} \| VT4$
$M4 = g^s \| g^t \| VT4 \| Sig_N(h3(g^s \| g^t \| VT4))$
Verifizieren von M4
Berechnen des Zwischenschlüssels $L := g^{tu}$
Entschlüsseln von VT4
CertU herausfinden
Überprüfen von id_N, g^s, IMUI und CertU anhand Revokationsliste
Berechnen eines dritten Terms = $g^t \| g^s \| id_N$
Berechnen eines Netzzertifikats CertN := dritter Term $\| Sig_{CA}$(h4(dritter Term))
Kreieren eines Zeitstempels TS
A

FIG 6a

FIG 6b


A
Berechnen eines fünften Terms TS || id_N || CertU
Berechnen eines zweiten signierten Terms = fünfter Term || Sig_{CA}(h4(fünfter Term))
M5 = CertN || zweiter signierter Term
Verifizieren von CertN und des zweiten signierten Terms
Berechnen eines vierten Terms := g^S || SigCA(h4(fünfter Term))
Generierung einer zweiten Zufallszahl r
Berechnen des Sitzungsschlüssels K := h1($(g^t)^s$ || r)
Berechnen einer Antwort A A := Enc (K, const)
M2 = r || A || vierter Term || dat1
Verifizieren von CertN
Berechnen des Sitzungsschlüssels K := h1($(g^s)^t$ || r)
Überprüfen der Antwort A
Berechnen eines ersten verschlüsselten Terms VT1 := Enc(K, Sig_U(h2(K || dat1 || dat2)))
Berechnen eines dritten verschlüsselten Terms VT3 := Enc (K, dat2)
M3 = VT1 || VT3
Entschlüsseln von VT1 und VT3
Verifizieren von SigU(h2(K || data1 || data2))

INTERNATIONAL SEARCH REPORT

International Application No
PCT/DE 96/00835

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	IEE PROCEEDINGS-COMPUTERS AND DIGITAL TECHNIQUES, MAY 1994, UK, vol. 141, no. 3, ISSN 1350-2387, pages 193-195, XP000454518 HARN L: "Public-key cryptosystem design based on factoring and discrete logarithms" see page 194, left-hand column, line 27 - line 42 --- -/--	1

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
4 October 1996	17. 10. 96

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+ 31-70) 340-3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/DE 96/00835

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	IEEE IN HOUSTON. GLOBECOM '93. IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE, INCLUDING A COMMUNICATIONS THEORY MINI-CONFERENCE. TECHNICAL PROGRAM CONFERENCE RECORD (CAT. NO.93CH3250-8), PROCEEDINGS OF GLOBECOM '93. IEEE GLOBAL TELECOMMUNICATIONS CONFERE, ISBN 0-7803-0917-0, 1993, NEW YORK, NY, USA, IEEE, USA, pages 164-170 vol.1, XP000428048 TSUBAKIYAMA H ET AL: "Security for information data broadcasting system with conditional-access control" see page 165, right-hand column, paragraph 1 ---	1
Y	EP,A,0 307 627 (ASCOM RADIOCOM AG) 22 March 1989 see column 4, line 48 - column 5, line 19 see column 7, line 42 - column 8, line 10 ---	1
A	IEEE PERSONAL COMMUNICATIONS, 1994, USA, vol. 1, no. 1, ISSN 1070-9916, pages 25-31, XP000460718 AZIZ A ET AL: "Privacy and authentication for wireless local area networks" see page 26, left-hand column, line 13 - page 27, right-hand column, line 28 see page 28, left-hand column, line 17 - line 24 ---	1-4
A	EP,A,0 460 538 (TOSHIBA) 11 December 1991 see column 7, line 40 - column 8, line 15 -----	11

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/DE 96/00835

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP-A-0307627	22-03-89	DE-A-	3870558	04-06-92
EP-A-460538	11-12-91	JP-A-	4037341	07-02-92
		EP-A-	0735723	02-10-96
		JP-A-	4297156	21-10-92
		US-A-	5136642	04-08-92
		JP-A-	4347949	03-12-92

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE 96/00835

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 H04L9/08

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	IEE PROCEEDINGS-COMPUTERS AND DIGITAL TECHNIQUES, MAY 1994, UK, Bd. 141, Nr. 3, ISSN 1350-2387, Seiten 193-195, XP000454518 HARN L: "Public-key cryptosystem design based on factoring and discrete logarithms" siehe Seite 194, linke Spalte, Zeile 27 - Zeile 42 --- -/--	1

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
4.Oktober 1996	17. 10. 96

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	Holper, G

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

C(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	IEEE IN HOUSTON. GLOBECOM '93. IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE, INCLUDING A COMMUNICATIONS THEORY MINI-CONFERENCE. TECHNICAL PROGRAM CONFERENCE RECORD (CAT. NO.93CH3250-8), PROCEEDINGS OF GLOBECOM '93. IEEE GLOBAL TELECOMMUNICATIONS CONFERE, ISBN 0-7803-0917-0, 1993, NEW YORK, NY, USA, IEEE, USA, Seiten 164-170 vol.1, XP000428048 TSUBAKIYAMA H ET AL: "Security for information data broadcasting system with conditional-access control" siehe Seite 165, rechte Spalte, Absatz 1 ---	1
Y	EP,A,0 307 627 (ASCOM RADIOCOM AG) 22.März 1989 siehe Spalte 4, Zeile 48 - Spalte 5, Zeile 19 siehe Spalte 7, Zeile 42 - Spalte 8, Zeile 10 ---	1
A	IEEE PERSONAL COMMUNICATIONS, 1994, USA, Bd. 1, Nr. 1, ISSN 1070-9916, Seiten 25-31, XP000460718 AZIZ A ET AL: "Privacy and authentication for wireless local area networks" siehe Seite 26, linke Spalte, Zeile 13 - Seite 27, rechte Spalte, Zeile 28 siehe Seite 28, linke Spalte, Zeile 17 - Zeile 24 ---	1-4
A	EP,A,0 460 538 (TOSHIBA) 11.Dezember 1991 siehe Spalte 7, Zeile 40 - Spalte 8, Zeile 15 -----	11

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/DE 96/00835

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
EP-A-0307627	22-03-89	DE-A-	3870558	04-06-92
EP-A-460538	11-12-91	JP-A-	4037341	07-02-92
		EP-A-	0735723	02-10-96
		JP-A-	4297156	21-10-92
		US-A-	5136642	04-08-92
		JP-A-	4347949	03-12-92

DOCKET NO: GR 98 P 1764 P
SERIAL NO: 09/700,928
APPLICANT: Horn et al.

LERNER AND GREENBERG P.A.
P.O. BOX 2480
HOLLYWOOD, FLORIDA 33022
TEL. (954) 925-1100

THIS PAGE BLANK (USPTO)